

COLEGIO DE JURISPRUDENCIA
UNIVERSIDAD SAN FRANCISCO DE QUITO

REGULACIÓN DE INTERNET Y DERECHOS DIGITALES EN ECUADOR



Juan Pablo Albán Alencastro - Valeria Betancourt - Hugo Cahueñas Muñoz - Arturo J. Carrillo
Andrés Delgado-Ron - Sophia Espinosa Coloma - Gustavo Gómez - Pier Pigozzi
Javier Robalino Orellana - Daniela Salazar Marín - Juan Carlos Solines Moreno
Farith Simon C. - Alfredo Velazco - Vladimir Villalba Paredes - Daniela Viteri

EDITORIAL USFQ - COLECCIÓN IURIS DICTIO
2016

REGULACIÓN DE INTERNET

Y

DERECHOS DIGITALES EN ECUADOR

Catalogación en la fuente. Biblioteca Universidad San Francisco de Quito

Regulación de Internet y derechos digitales en Ecuador / Juan Pablo Albán Alencastro … [y otros catorce] ; editoras generales, Daniela Salazar, Daniela Viteri. – Quito : Editorial USFQ, 2016.
p. : il.

Incluye referencias bibliográficas
ISBN: 978-9978-68-097-1

1. Internet – Legislación – Ecuador. – 2. Propiedad intelectual – Internet – Ecuador. – 3. Tecnología de la información – Legislación – Ecuador. – 4. Protección de datos – Legislación – Ecuador. – 5. Comercio electrónico – Legislación – Ecuador. – I. Albán Alencastro, Juan Pablo. – II. Salazar, Daniela, ed. – III. Viteri, Daniela, ed.

LC: KHK 335 .C45 R34 2016 CDD: 343.866 099 44

EDITORIAL USFQ - LINEA IURIS DICTIO - 2016
Universidad San Francisco de Quito
Campus Cumbayá USFQ, Quito 170901, Ecuador. http://editorial.usfq.edu.ec

La Editorial USFQ es un departamento de la Universidad San Francisco de Quito USFQ que fomenta la misión de la Universidad al diseminar el conocimiento para formar, educar, investigar y servir a la comunidad dentro de la filosofía de las Artes Liberales.

Regulación de Internet y Derechos Digitales en Ecuador

Autores: Juan Pablo Albán Alencastro, Valeria Betancourt, Hugo Cahueñas Muñoz, Arturo J. Carrillo, Andrés Delgado-Ron, Sophia Espinosa Coloma, Gustavo Gómez, Pier Pigozzi, Javier Robalino Orellana, Daniela Salazar Marín, Juan Carlos Solines Moreno, Farith Simon C., Alfredo Velazco, Vladimir Villalba Paredes, Daniela Viteri

Editoras Generales: Daniela Salazar Marín, Daniela Viteri
Comité Editorial: Luis Parraguez Ruiz; Hugo García Larriva; Oswaldo Santos Dávalos; José Irigoyen (Comisión de Publicaciones, Colegio de Jurisprudencia USFQ)

Esta obra es publicada luego de un proceso de revisión por pares (*peer-reviewed*) que contó con la participación de los siguientes revisores académicos: Efrén Guerrero Salgado (Pontificia Universidad Católica, Quito, Ecuador) y José Luis Barzallo (Pontificia Universidad Católica, Quito, Ecuador).

Producción Editorial: María José Valencia-Argüello; Diego F. Cisneros-Heredia (Editorial USFQ)
Diagramación y portada: Edwin Fuentes (Departamento de Diseño Editorial USFQ)
Revisión de estilo e idioma: Gabriela Michelena Otero (Departamento de Composición USFQ)

Esta obra se publica gracias al apoyo financiero de Google Inc.

Diciembre 2016, Quito

Impreso en Ecuador por Prodedim - *Printed in Ecuador*
Publicado en línea en el portal web de la Editorial USFQ: http://editorial.usfq.edu.ec
USFQ: http://libros.usfq.edu.ec/

ISBN: 978-9978-68-097-1

TABLA DE CONTENIDOS

PRESENTACIÓN

Esta publicación nace de la necesidad de comprender y analizar la regulación del internet en Ecuador. Las tecnologías de la información y comunicación (TICs) están avanzando de manera vertiginosa sin que el derecho se haya adaptado con suficiente rapidez a los cambios tecnológicos. Si bien en Ecuador se han aprobado distintas normas que abordan algunos aspectos del internet, no hemos reflexionado suficiente sobre las respuestas que el derecho ecuatoriano ha ofrecido a este fenómeno, ni sobre los vacíos legales que aún existen. Desde el ámbito académico, todavía no existen respuestas definitivas a preguntas como: ¿Qué áreas del derecho requieren regulación de la actividad en internet? ¿Qué tipo de regulación es la más adecuada? o ¿Para qué fines debe regularse internet? De ahí nuestro interés en motivar una reflexión sobre la regulación del internet y la situación de los derechos digitales en Ecuador.

Dada la diversidad de materias que están vinculadas con el uso de internet, consideramos necesario conformar un equipo interdisciplinario de académicos capaces de abordar la regulación de internet en sus distintos frentes. Ahora bien, la reflexión académica no puede estar aislada de la labor que realizan las organizaciones de la sociedad civil para defender los derechos digitales en internet. Es por ello que en esta publicación la compilación de artículos está dividida en dos partes. La primera parte agrupa artículos de la academia y la segunda parte agrupa artículos de la sociedad civil.

Para la *primera parte*, convocamos a abogados y docentes especialistas en derechos humanos, derecho de las nuevas tecnologías, derecho penal, derechos de la niñez y la adolescencia, derecho administrativo, derecho de las telecomunicaciones, derecho mercantil, derechos de autor, entre otras áreas de especialización. Los artículos no constituyen contribuciones realizadas de manera individual por cada investigador sino que son el fruto de una jornada de reflexión colectiva en la que cada uno de los autores tuvo la oportunidad de presentar su investigación y recibir comentarios de los otros autores, así como de expertos en el área.

Para la *segunda parte*, convocamos a defensores de internet y derechos digitales en Ecuador y les invitamos a participar de un panel que se celebró el 24 de mayo de 2016 en la Universidad San Francisco de Quito. En el marco de este evento público, los principales exponentes de la sociedad civil presentaron su visión sobre la regulación de internet en Ecuador y los académicos escucharon sus preocupaciones así como los desafíos que enfrentan para defender un internet libre en Ecuador. Las reflexiones presentadas por la sociedad civil fueron tan valiosas que encontramos indispensable incluir sus ponencias como parte de esta publicación. Desde nuestra visión, si esta compilación de artículos pretende ser útil, debe reflejar y propiciar

el diálogo entre la academia y los actores fundamentales de la gobernanza de internet en Ecuador.

Finalmente, en el proceso de elaboración de esta publicación, la Asamblea Nacional inició el debate de un nuevo proyecto de ley respecto de la protección de datos personales que incluye varios aspectos regulatorios del internet. Esta publicación no estaría completa sin un análisis del proyecto, por lo que fue necesario incluir una *tercera parte* con los resultados de un seminario dedicado a estudiar los desafíos de la reglamentación sobre protección de datos para Ecuador y la promoción del comercio electrónico y los negocios sobre Internet, llevado a cabo el 8 de septiembre de 2016 en la Universidad San Francisco de Quito.

Esta publicación no pretende ser una solución definitiva a los desafíos del marco jurídico que regula el internet en Ecuador, no obstante, estamos convencidas de que constituye un insumo fundamental para los debates de políticas públicas y proyectos legislativos que se discuten en la actualidad. Nuestro interés es que los artículos constituyan un insumo para organizaciones de la sociedad civil, universidades, legisladores y tomadores de decisión involucrados en estas discusiones.

Si bien esta compilación de artículos está enfocada en la regulación en Ecuador, su objetivo es hacer una contribución a los debates que tienen lugar en toda la región. En ese sentido, entre los autores se encuentran también expertos internacionales que permiten ofrecer una mirada comparada a esta temática. Destacamos que la publicación tiene un enfoque de derechos humanos pues partimos del convencimiento de que toda intervención del Estado en materia de internet debe realizarse en respeto de los derechos digitales.

Esta publicación, la primera de su género en Ecuador, ha sido realizada gracias al apoyo financiero de Google Inc. en el marco de un proyecto desarrollado por el Colegio de Jurisprudencia de la Universidad San Francisco de Quito. Esperamos que los lectores encuentren este aporte tan enriquecedor y útil como nosotras.

Daniela Salazar Marín, Daniela Viteri
Editoras generales

PRÓLOGO

Internet se va convirtiendo en una de las principales plataformas de información y comunicación de las sociedades modernas y, por tanto, en soporte para el ejercicio de derechos fundamentales como la libertad de expresión y el derecho a la información, entre otros. En este nuevo entorno digital, el acceso a Internet se convierte en un derecho en sí mismo y una obligación que el Estado debe asumir, de forma que nadie quede excluido de sus beneficios.

No hay país en el mundo donde no se esté debatiendo sobre Internet, y evaluando su impacto en la economía, la sociedad y el desarrollo nacional. Ecuador no es la excepción. Parte de los debates actuales refieren a la necesidad, o no, de regularlo. Pero lo cierto es que Internet está regulado desde sus inicios, y lo es actualmente, tanto en Ecuador como en resto del mundo. Mal o bien, por Estados autoritarios o por Estados democráticos, pero regulado.

De ahí que el debate urgente sea determinar cómo se regula, cuáles son límites legítimos (y cuáles no) a su uso, y quién aplica esa regulación, para que la intervención estatal sea verdadera garantía de libertad y no una forma de censura encubierta.

Cualquier esfuerzo en este sentido deberá encararse desde una perspectiva desde los derechos humanos. Y esa mirada no sólo está en el título sino que está incluida en toda la obra, y la ha motivado.

El libro **"Regulación de Internet y Derechos Digitales en Ecuador"** se convierte en un aporte novedoso e invalorable en el actual contexto ecuatoriano, destinado a aportar insumos de alto nivel profesional, que seguramente será bienvenido por académicos, así como organizaciones de la sociedad civil, instituciones educativas, periodistas, empresarios del sector, reguladores y autoridades estatales.

Novedoso, porque la Universidad de San Francisco se propuso publicar un ambicioso libro sobre un asunto de interés público sobre el que aún faltan información, análisis y diálogo, para poder encontrar las respuestas a los desafíos que Internet nos ha puesto frente a nuestras narices.

E invalorable, porque se encuentran aquí aportes que abarcan la diversidad de temas que Internet propone y desafía, realizados desde diversas perspectivas y de opiniones por especialistas de distintas disciplinas. Autores que nos han omitido abordar aspectos complejos, sensibles e incluso polémicos, como los relativos a las evidentes tensiones entre derechos de igual rango como los que existen entre la libertad de expresión y la libertad de religión, y entre aquella y los derechos de

niños, niñas y adolescentes; o el conflicto entre el derecho a la información y los derechos a la imagen o los derechos de autor.

No tengo ninguna duda que los artículos que usted encontrará acá, esté de acuerdo o no con lo que expresan, serán una referencia fundamental no sólo para el análisis de la situación actual en Ecuador sino también para la búsqueda de caminos democráticos que garanticen una Internet libre y abierta, y la plena vigencia de los derechos digitales de todas y todos los ecuatorianos.

....

El libro incluye artículos, ubicados en perfecto orden alfabético, de Juan Pablo Albán Alencastro, Hugo Cahueñas Muñoz, Arturo J. Carrillo, Sophia Espinosa Coloma, Pier Pigozzi, Javier Robalino Orellana, Daniela Salazar Marín, Juan Carlos Solines Moreno, Farith Simon C., y Vladimir Villalba Paredes. También se incluyeron aportes de organizaciones sociales que fueron presentados en el Foro "Sociedad Civil y Derechos Digitales". Los mismos corresponden a Valeria Betancourt (APC), Andrés Delgado (Apertura Radical), Alfredo Velazco (Derechos Digitales) y Daniela Viteri (Observatorio para la Juventud para América Latina y el Caribe).

La aplicación del derecho penal en Internet es el motivo central del primer artículo del libro, redactado por **Juan Pablo Albán Alencastro**. De manera sistemática y profunda, se expone la experiencia comparada a nivel internacional en materia de delitos informáticos y ciberdelincuencia, en tanto Internet brinda oportunidades para cometer delitos que se pueden realizar por otros medios y que ya están tipificados en la legislación actual. Asimismo, se aportan insumos provistos desde los estándares interamericanos de libertad de expresión para orientar la política criminal en materia de cibercrímenes.

En "**¡Punir o no punir, esa es la cuestión! (el derecho penal ecuatoriano y la sociedad de la información)**" se analiza la normativa ecuatoriana en materia de cibercrímenes a partir de la aprobación del Código Orgánico Integral Penal de 2014, describiendo los tipos penales que podrían ser considerados como tales y los bienes jurídicos que protegen.

Desde la comprensión que la regulación estatal se ha hecho necesaria, el autor expone una visión crítica sobre la pertinencia y conveniencia de la tipificación penal para algunos de los abusos cometidos en Internet, tanto como frente a la forma que la normativa ecuatoriana responde a los desafíos de la era digital en la materia. Entre otros, para resolver los problemas en la persecución penal de dichos delitos, en aspectos tales como la responsabilidad, la territorialidad, la jurisdicción aplicable y el anonimato, entre otros.

El artículo sobre **"Las telecomunicaciones en desastres: el deber de facilitar y proteger el uso del Internet"** de **Hugo Cahueñas Muñoz** expone la importancia que las telecomunicaciones y una Internet accesibles y robustas tienen ante situa-

ciones de catástrofes, tales como los terremotos, ya sea antes del evento, durante el mismo y en la recuperación posterior.

Además de recoger el derecho comparado, las experiencias de países vecinos y los estándares y recomendaciones internacionales (por ejemplo el Convenio de Tampere) en relación al uso de las telecomunicaciones en situaciones de desastre, el autor desarrolla un prolijo diagnóstico de la normativa de Ecuador y analiza la respuesta del sector de las telecomunicaciones en una situación reciente e ineludible: el terremoto ocurrido en abril de 2016.

Finalmente, propone a los lectores y actores involucrados una serie de conclusiones y recomendaciones de ajustes regulatorios así como planes y medidas que se deberían adoptar para mejorar la respuesta nacional ante futuros desastres, utilizando toda la capacidad de las telecomunicaciones y optimizando el uso de las redes, servicios y aplicaciones disponibles en Internet como herramientas fundamentales para gestionar.

Arturo J. Carrillo aborda un tema de candente actualidad en el mundo, como es la **"Protección a la neutralidad de la red en Ecuador a la luz del derecho internacional"**, analizando hasta dónde la legislación ecuatoriana respeta este principio de no discriminación y cumple con sus obligaciones internacionales en la materia.

Para ello, el autor desarrolla los parámetros pertinentes establecidos por el derecho internacional de los derechos humanos, ya sea a partir de tratados internacionales de aplicación obligatoria para el país, como de estándares elaborados por organismos especializados del Sistema Interamericano de Derechos Humanos como la Relatoría Especial para la Libertad de Expresión, entre otros.

El artículo incluye un análisis sobre la Ley Orgánica de Telecomunicaciones y su impacto en la neutralidad de la red, así como de las estrategias desarrolladas por operadores de telecomunicaciones y proveedores de servicios de Internet a la luz de esa normativa, como los planes de *zero-rating*.

La **"Regulación de propiedad intelectual en Internet: la paradoja del siglo XXI"** es el artículo que nos presenta **Sophia Espinosa Coloma**, proponiendo el análisis del papel de los derechos de propiedad intelectual (y su regulación) en un nuevo entorno digital, donde los negocios y el valor de mercado de las empresas se basan en activos intangibles y en las creaciones del intelecto humano: la economía del conocimiento.

Dentro de los derechos de propiedad intelectual, la autora opta por describir las características del derecho de autor, la normativa internacional aplicable y su

papel en Internet, explorando la legislación de Ecuador al respecto, así como proyectos a estudio (como el Código Orgánico de Economía Social del Conocimiento e Innovación o Código Ingenios), y presentando conclusiones de cuáles serían los mejores caminos para una regulación del derecho de autor en el entorno digital.

Un aporte distintivo del artículo se encuentra en presentar las tensiones con otros derechos reconocidos en el país, como los de acceso al conocimiento y a la información, tomando, como uno de sus ejemplos, la utilización de la protección de derechos de autor para prohibir el uso de contenidos e imágenes relacionadas con el Presidente de la República.

Esta obra incluye un inquietante y apasionante tema, que muchas veces parece lejano a nuestra región, pero que **Pier Pigozzi** propone analizar para aprender de qué manera regular el uso y acceso a Internet, en especial cuando se trata de equilibrar el ejercicio de derechos y libertades que pueden contraponerse. Se trata de "**La insuficiencia de la regulación: lecciones para el Internet a partir de la desregulación de la blasfemia".**

El artículo despliega amplia información y análisis sobre las tensiones entre la libertad de expresión y la libertad de religión en el mundo, dos derechos reconocidos internacionalmente con el mismo nivel, tomando como eje el debate y tratamiento regulatorio de la "blasfemia", en particular en la experiencia internacional.

Pero es a partir de este tema, que el autor desarrolla su perspectiva sobre el debate sobre la regulación en Internet, una alerta ante los riesgos de censura arbitraria y otras formas de violación a esas libertades que algunos procesos regulatorios traen aparejados y, más profundamente, sobre su visión respecto a la regulación en general como mecanismo ineficaz e insuficiente para resolver tensiones entre derechos fundamentales.

La rica diversidad de artículos de este libro también da lugar a otro de los desafíos de la economía digital, el ingreso de tecnologías disruptivas que crean nuevos mercados y nuevos consumidores.

Este aspecto de la regulación en Internet es abordado por **Javier Robalino Orellana** en su artículo "**Respuesta administrativa a los derechos sociales. Especial énfasis en las tecnologías disruptivas".**

El autor describe cuál debería ser la respuesta y las obligaciones estatales (es decir, regulación) con relación a las tecnologías disruptivas -entendidas como nuevas tecnologías o innovaciones que presentan menores costos y una mejor performance para los negocios en el entorno digital- tomando en cuenta los derechos humanos y constitucionales que han sido garantizados por el propio Estado a sus ciudadanos y consumidores.

La Ley Orgánica de Comunicación (LOC) aprobada en 2013 no regula la información u opinión que de modo personal se emita a través de Internet de su amplio alcance, pero para **Daniela Salazar Marín** esta norma ha tenido un impacto perjudicial en la libertad de expresión de los ecuatorianos a través de Internet.

El artículo denominado **"El impacto de la Ley Orgánica de Comunicación en la libertad de expresarnos a través de Internet en Ecuador**" es un análisis en profundidad del texto legal donde se fundamenta por qué razones se entiende que algunas disposiciones de la misma han tenido un impacto amplio y nocivo en el derecho a expresión en el entorno digital.

La inclusión de los portales web de los medios tradicionales en el alcance de la LOC, los incentivos para que éstos y otros intermediarios se conviertan en censores privados de los comentarios que terceras personas publican a través de los portales de Internet de tales medios, así como la aplicabilidad del derecho de rectificación y la desprotección del derecho al anonimato en Internet son algunos de los aspectos que la autora propone considerar para concluir que no existe un marco regulatorio adecuado para garantizar la libertad de expresión a través de Internet en Ecuador.

Internet y, en general, las tecnologías de información y comunicación (TIC), se han convertido en un elemento central en la cultura de las nuevas generaciones, que participan en ellas ya sea como receptores pasivos, como creadores o como activos usuarios que procesan y comparten contenidos. Así comienza el artículo de **Farith Simon C.**, que expone los riesgos, pero también las oportunidades, para los niños, niñas y adolescentes ecuatorianos en este nuevo escenario mediático.

"Internet y la niñez y adolescencia en el Ecuador: una mirada general al estado de la cuestión" expone una cita de estudios y datos sobre estas cuestiones, además de recoger la legislación internacional de referencia y un extenso relevamiento de la legislación nacional en la materia. El autor no olvida un repaso esencial sobre el enfoque de derechos que debería primar a la hora de aprobar políticas públicas y normativas referidas al acceso y uso del Internet.

Finalmente, además del análisis mencionado, desarrolla una serie de conclusiones y recomendaciones con insumos para superar ausencias o limitaciones de las políticas públicas y normativas actuales sobre los derechos de niños, niñas y adolescentes en Internet y las TIC.

"Telecomunicaciones e Internet en Ecuador del siglo XXI: apuntes técnicos, historia reciente y la ruta hacia el control de usuarios y contenidos" describe profusamente las características y datos sobre el fuerte desarrollo que, en el marco de un proceso de apertura y liberalización, ha tenido la industria de las telecomunicaciones en la economía y sociedad actual.

Complementariamente, explica de manera didáctica cuál es la infraestructura, las características técnicas y económicas de las telecomunicaciones, y el andamiaje jurídico y regulatorio que soporta Internet y permite su acceso y uso por parte de las personas.

Para su autor, **Juan Carlos Solines Moreno**, sin embargo, el empoderamiento de la sociedad gracias a un crecimiento de los flujos de información y una notoria influencia de las redes sociales están bajo riesgo de influencias gubernamentales en el sector de las telecomunicaciones que pueden afectar adversamente a derechos fundamentales y al desarrollo de la Sociedad de la Información en Ecuador. Entre otros aspectos, el autor menciona evidencias de una estrategia estatal de regulación, un modelo de diseño institucional y ciertas políticas públicas que se orientarían al control de usuarios y contenidos.

Un aspecto relevante de la nueva economía digital refiere al comercio electrónico y las garantías en el régimen de contratación, las firmas electrónicas y otros aspectos que hacen tanto a los negocios entre empresas, como a la debida protección de los consumidores.

En el último artículo del libro, denominado **"Régimen de contratación privada en Internet, una aproximación local"**, **Vladimir Villalba** aporta detallados elementos al respecto de la legislación vigente en Ecuador (Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos y Ley Orgánica de Defensa del Consumidor, entre otras) abordando temas tales como el fenómeno de la autenticidad y prueba del contrato, el contenido de la oferta, la autenticidad del sujeto, los medios de pago y diversas cuestiones referidas a las acciones frente a posibles incumplimientos.

Gustavo Gómez Germano
Director Ejecutivo
Observatorio Latinoamericano de Regulación, Medios y Convergencia
OBSERVACOM

PRIMERA PARTE
ENSAYOS ACADÉMICOS

¡Punir o no punir, esa es la cuestión! (el derecho penal ecuatoriano y la sociedad de la información)

Juan Pablo Albán Alencastro
Universidad San Francisco de Quito

RESUMEN: Resultado del desarrollo tecnológico informático existe una proliferación de delitos informáticos que vulneran la intimidad de los individuos y la seguridad de las instituciones públicas y privadas. El Código Orgánico Integral Penal ha tornado complejo el reto de "criminalizar" los conflictos sociales que surgen por el uso de internet.

PALABRAS CLAVE: cibercrímenes, internet, COIP, derechos digitales, delitos, persecución penal

ABSTRACT: Technological development conveys a proliferation of digital crimes that violate the privacy of individuals and the security of public and private institutions. The new Criminal Code has turned complex the challenge of "criminalizing" social conflicts that arise from the use of internet.

KEYWORDS: cybercrimes, internet, Criminal Code, digital rights, crimes, criminal persecution

1. Política criminal a la ecuatoriana

La potestad punitiva, como atributo de la soberanía estatal, no puede ser ejercida legítimamente sin una justificación política que, entre otras cosas, implica la identificación de los valores que deben ser preservados en la sociedad, una clara definición del objeto, alcance y fines perseguidos por los mecanismos de control social reactivo y formal a través del derecho penal y, en general, la fijación de una postura del Estado frente al fenómeno delictivo.

En palabras de Juan Bustos y Hernán Hormazábal, "[f]rente a un conflicto social, el Estado social y democrático de derecho debe antes que nada desarrollar una política social que conduzca a su prevención o solución o, en último término, pero sólo en último término, optar por definirlo como criminal" (Bustos y Hormazábal, 1997 p. 29).

Esto exige una ingeniería penal ajustada a la realidad e idiosincrasia de cada grupo social, coherente con el diseño constitucional y las obligaciones internacionales del Estado en materia de Derechos Humanos y estable, lo que no es sinónimo de inmutable, sino, más bien, de predecible y razonable.[1]

Lamentablemente, a través de toda su historia, el modelo penal ecuatoriano ha carecido de una política criminal definida. De hecho, en mi opinión, las decisiones del Estado ecuatoriano en materia de política criminal se han caracterizado por la improvisación o, si se quiere, por la novelería. Las acciones legislativas y de política pública emprendidas para enfrentar el delito han dependido, en general, del rédito electoral que en determinado momento histórico podría reportar una postura de mano dura o de mano blanda frente a ciertas modalidades delictivas, sin pensar en las víctimas ni en los reos[2]. No ha habido mayor reflexión sobre la verdadera conveniencia desde el punto de vista social para introducir nuevas figuras penales, suprimir otras, aumentar o reducir penas, etc.

Sobre esta cuestión dice el Maestro Ernesto Albán Gómez:

> [d]urante la vigencia de la codificación de 1971, hasta su derogatoria el 2014, se produjeron cuarenta y seis reformas referidas a materias muy diversas, con novedades introducidas sin la debida coherencia con el resto de normas; algunas de ellas caracterizadas por lo inconsulto, apresurado y anti técnico, y motivadas en varios casos por circunstancias coyunturales y no exentas de demagogia política (Albán Gómez, 2015, p. 57).

---

1 El hecho de que un Estado mantenga un modelo penal a través del tiempo para garantizar certeza jurídica a los ciudadanos no significa que no deba revisarse atendiendo a las nuevas exigencias y realidades del fenómeno delincuencial, sino que no debe tomar por sorpresa a quienes eventualmente serán sometidos a él.

2 Pudiera hacerse alusión a la diferencia entre el Plan Nacional del Buen Vivir 2009-2013 (pag. 306 por ej.) y el Plan Nacional del Buen Vivir 2013-2017 (pág 201 por ej).

Tal vez el mejor ejemplo de esta situación nos lo dio el actual régimen con la reforma penal en materia de drogas que supuestamente apuntaba a una progresiva legalización del consumo y microtráfico, seguida pocos meses después de una contrarreforma que a todas luces busca criminalizar la pobreza y el ejercicio del derecho al libre desarrollo de la personalidad.

Cuando se trata de ámbitos novedosos y, por ende, desconocidos como las nuevas tecnologías de la información, la reacción ecuatoriana frente a su potencial es o bien muy tardía o bien poco reflexiva y demasiado apresurada, por lo tanto, en muchas ocasiones inadecuada. Esto vuelve aún más complejo el reto de "criminalizar" los conflictos sociales que surgen por el uso de Internet, pues el objeto de tal tarea es voluble y cambiante, pero además lo es a una velocidad que saca notable ventaja a la técnica y desarrollo normativos.

Por otra parte, nuestro diseño constitucional se sostiene en la filosofía garantista, por lo tanto, corresponde un modelo penal de mínima intervención en que el catálogo de conductas penalmente reprochables debe restringirse a lo estrictamente indispensable y el legislador debe resistirse a la tentación de punir a menos que tenga razones de peso para castigar determinada conducta que no se había contemplado anteriormente como delictiva.

Además, está el problema de la interpretación de las normas penales que debe realizarse en forma estricta, literal y sin extender sus contenidos a situaciones que originalmente el legislador no haya previsto, por lo que la solución propuesta por autores como Andrés Díaz Gómez, frente a las nuevas posibilidades que ofrece Internet para poner en riesgo o dañar ciertos bienes jurídicos o simplemente interpretar tipos penales preexistentes es, por decir lo menos, problemática.

Es en este escenario donde vamos a examinar la respuesta ecuatoriana a los denominados cibercrímenes.

2. Derecho penal e Internet: la experiencia internacional y comparada

Tal vez la virtud mayor de Internet es ser un espacio donde se privilegia la libertad y se procura reducir al máximo posible las restricciones de su acceso y uso. En palabras de Rodríguez: "[e]n un primer momento se entendió que el Ciberespacio configuraba un territorio que era esencialmente libre, que no era susceptible de ser gobernado y, por tanto, ajeno a todo control y resistente frente a cualquier influjo dominador" (Rodríguez-Magariños, 2008, p. 1).

Sobre esta misma cuestión dice Paula López Zamora, Profesora de la Universidad Complutense, que el Ciberespacio implica una ausencia de control o al menos así es como fue ideado, por eso se afirma que Internet es "el paradigma de la libertad; un mundo en que los controles convencionales no sirven para nada y donde no

existe jerarquía. Querer regular Internet, se dice, es como querer regular el tiempo" (López Zamora, 2006, p. 96).

Pero simultáneamente,

> "En el Ciberespacio se implementan multitud de servicios que van transformando nuestros usos y costumbres, prestaciones que se fundamentan en la gran capacidad de comunicación que nos ofrece la red. Trata también servicios como la tele-educación (*e-learning*), el comercio electrónico (*e-commerce*) o la administración electrónica (*e-government*), la telemedicina (*e-health*), la gestión electrónica de recursos para empresas (*e-management*), la banca telemática (*home-banking*), el teletrabajo (*tele-work*), la oferta publicitaria (*cibermarketing*) o más directamente en el ámbito de la gestión de esfera doméstica (la domótica)."(Rodríguez-Magariños, 2008, p. 2).

Y precisamente por esa versatilidad y diversidad de usos y aplicaciones que el Internet ofrece (cada vez más y con mayor frecuencia) y por la expansión de la red para abarcar todo tipo de información pública y privada con la consecuente expropiación progresiva de nuestros datos, eventualmente se volvió impostergable la intromisión del Estado y su derecho de castigar conductas cometidas en o a través del Internet que a los ojos del colectivo social son desviadas, dañosas o riesgosas.

Aunque la temática del presente artículo es más amplia, a continuación examinaremos de manera general algunos hitos del desarrollo internacional y comparado en el combate a la ciberdelincuencia.

En el plano internacional se han dado iniciativas de *soft law*, tendientes a que los Estados actualicen su legislación para abordar la problemática de la cibercriminalidad, vale destacar, por ejemplo, los esfuerzos realizados por la Organización para la Cooperación y el Desarrollo Económicos en Europa (OCDE) desde 1983, cuando emprendió un estudio sobre la posibilidad de aplicar y armonizar en el plano internacional las leyes penales, a fin de luchar contra el problema del uso indebido de los programas de computación; todo este esfuerzo concluyó con la publicación, en 1986, del informe titulado "Delitos de Informática" que examina el marco jurídico entonces vigente en diversos países europeos, marco que potencialmente podía ser utilizado para enfrentar esta forma de criminalidad, así como una serie de propuestas mínimas de reforma y ampliación a partir de ejemplos de uso indebido de sistemas informáticos que los países podrían prohibir mediante el derecho penal, por ejemplo, el fraude y la falsificación informática, la alteración de datos, el acceso no autorizado, la interceptación y la reproducción no autorizada de programas y aplicaciones.

También el Consejo de Europa desde 1996[3] a través de su Legal Advisory Board y desde 1997 con el Plan de Acción adoptado por los Jefes de Estado y de Gobierno del Consejo de Europa con ocasión de su Segunda Cumbre (Estrasburgo, 10 y 11 de octubre de 1997), empezó a desarrollar una estrategia para buscar respuestas comunes ante la proliferación de las nuevas tecnologías de la información. Tales esfuerzos llegaron a un consenso, en abril de 2000, y se publicó el "Proyecto de Convención sobre el Delito Cibernético", cuyos aspectos técnicos fueron afinados por un grupo de expertos en diciembre del mismo año, con lo que se llamó la atención del Comité de Ministros de Europa, institución que en noviembre de 2001 aprobó el Convenio sobre la Ciberdelincuencia, también conocido como Convenio de Budapest[4].

Entre los aspectos más notables del tratado en cuestión se encuentran: a) la promoción de la armonización del derecho penal sustantivo de los Estados miembros en materia de delitos cibernéticos; b) la propuesta de parámetros procesales mínimos para la investigación y sanción de tales conductas; c) la identificación de ciertas infracciones particularmente graves que deberían merecer atención prioritaria, a saber, las que implican violaciones a los derechos de autor, el fraude informático, la pornografía infantil, los delitos de odio y las violaciones de seguridad de las redes; y d) la creación de mecanismos de cooperación a nivel europeo para el combate a la ciberdelincuencia.

En nuestra región, la Organización de los Estados Americanos, en el marco de la Asamblea General del año 2003, adoptó la resolución AG/RES. 1939 (XXXIII-O/03) (Desarrollo de una Estrategia Interamericana para Combatir las Amenazas a la Seguridad Cibernética)[5] y destacó la necesidad de desarrollar una estrategia para la protección de las infraestructuras de información que adopte un enfoque integral, internacional y multidisciplinario. De hecho, en el mes de julio del mismo año 2003, se celebró una Conferencia de Seguridad Cibernética en Argentina, cuyo objetivo era identificar las amenazas a los sistemas de información esenciales, las infraestructuras esenciales y las economías no solo de los países de América, sino del mundo.

A partir de entonces, la Estrategia Interamericana Integral de Seguridad Cibernética ha sido desarrollada a través de tres organismos: el Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL) y la Reunión de Ministros de Justicia o Ministros o Procuradores Genera-

---

3 Legal Aspects of Computer-Related Crime in the Information Society, disponible en: http://www.echo.lu/legal/en/comcrime/sieber.html.

4Convenio sobre la Ciberdelincuencia, disponible en: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c.

5 AG/RES. 1939 (XXXIII-O/03), disponible en: http://www.oas.org/juridico/spanish/agres_1939.pdf.

les de las Américas (REMJA). La Estrategia reconoce la necesidad de que todos los participantes en las redes y sistemas de información sean conscientes de sus funciones y responsabilidades con respecto a la seguridad, a fin de crear una cultura de seguridad cibernética, lo que lamentablemente ha sido interpretado por ciertos actores como una permisión intergubernamental de híper regulación, inclusive a través de decisiones unilaterales de los proveedores de servicios o contenidos que terminan por perjudicar los derechos de los cibernautas.

Vale destacar, además, que la VI Conferencia de Ministros de Defensa de las Américas celebrada en el Ecuador en noviembre de 2004, resolvió promover el diálogo entre los Estados miembros de la OEA para la planificación de medidas preventivas, a fin de prevenir y responder a las amenazas terroristas emergentes, entre ellas, los cibercrímenes.

En el ámbito de Naciones Unidas, el Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en 1990, en La Habana, Cuba, concluyó que la delincuencia relacionada con la informática es la consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos. El congreso recomendó que se establecieran normas y directrices para la seguridad de las computadoras, a fin de auxiliar a la comunidad internacional a hacer frente a estas nuevas formas de delincuencia[6].

El Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente celebrado en Viena, en el año 2000, prestó particular atención a la lucha contra la delincuencia en Internet e incluyó un curso práctico organizado por el Instituto de las Naciones Unidas de Asia y el Lejano Oriente para la Prevención del Delito y el Tratamiento del Delincuente (UNAFEI), con sede en Tokyo, bajo los auspicios del Centro de las Naciones Unidas para la Prevención Internacional del Delito (CICP), centrado en la cooperación mundial para investigar y enjuiciar al delincuente cibernético[7].

La Convención de Naciones Unidas contra la Delincuencia Organizada Transnacional, vigente desde 2003, promueve en su artículo 29 la capacitación y asistencia técnica "para combatir la delincuencia organizada transnacional mediante computadoras, redes de telecomunicaciones u otras formas de la tecnología moderna"[8].

---

6 A/CONF,144/28/REV1, disponible en: https://www.unodc.org/documents/congress/Previous_Congresses/8th_Congress_1990/028_ACONF.144.28.Rev.1_Report_Eighth_United_Nations_Congress_on_the_Prevention_of_Crime_and_the_Treatment_of_Offenders_S.pdf.

7 Comunicado de prensa del Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, disponible en: http://www.un.org/es/conf/xcongreso/prensa/2088hs.shtml.

8 Convención de las Naciones Unidas contra la delincuencia organizada transnacional: disponible en: https://www.unodc.org/pdf/cld/TOCebook-s.pdf.

En cuanto a las respuestas dadas sobre el fenómeno de la cibercriminalidad por Estados particulares se puede destacar la incorporación de nuevos tipos específicos a los Códigos Penales de Alemania en 1986, Austria en 1987, Francia en 1988, Chile en 1993, Estados Unidos en 1994 (con la adopción de su Acta Federal de Abuso Computacional que modificó al Acta de Fraude y Abuso Computacional de 1986) y España en 1995.

El objetivo general perseguido en todos estos casos fue proteger a las personas, empresas y al propio Estado de la interferencia, daño y acceso no autorizado a bases de datos y sistemas computarizados creados legalmente. Esto porque el desarrollo tecnológico informático trajo consigo la proliferación de delitos informáticos y otras formas irregulares de acceso a las computadoras, sistemas y bases de datos comprometiendo la intimidad de los individuos y la seguridad de las instituciones financieras, otros negocios, agencias gubernamentales y otras relacionadas con el gobierno.

Específicamente, la ley alemana de agosto de 1986, en general, castiga conductas en las que el bien jurídico comprometido son precisamente las bases de datos informáticas o los datos en ellas alojados, por eso contiene tipos específicos que penalizan el espionaje, la alteración, la falsificación y el sabotaje informáticos, además de ciertas modalidades de fraude en las que el instrumento para la comisión del delito es un medio informático.

En Austria el objetivo principal de la ley de diciembre de 1987 es la protección de los datos personales y programas informáticos frente a su potencial destrucción. La ocasión fue también aprovechada para la tipificación de los fraudes informáticos.

La ley 88-19 de 5 de enero de 1988 de Francia se limita a desarrollar pautas para la investigación y persecución de los fraudes informáticos.

En el caso chileno, la Ley Nº 19.223 tiene como finalidad proteger a un nuevo bien jurídico como es: "la calidad, pureza e idoneidad de la información en cuanto a tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan".

El Acta de Abuso Computacional de 1994 en Estados Unidos castiga penalmente la transmisión de programas, información, códigos o comandos que causen daños a una computadora, al sistema informático, a las redes, información o los datos alojados en sistemas informáticos. El acta diferencia dos formas de comisión del hecho: una intencional que merece un castigo de hasta 10 años en prisión federal además de una multa y otra culposa para la cual la sanción oscila entre una simple multa y un año en prisión.

En España, el tratamiento del nuevo Código Penal de 1995, aprobado por Ley Orgánica 10/1995 de 23 de Noviembre del mismo año, incorpora delitos informáticos en estricto sentido (aquellos en que el bien jurídico protegido son justamente

los sistemas y datos informáticos) como la usurpación y cesión de datos, la intercepción de comunicaciones electrónicas o los daños informáticos y otros en los que el medio comisivo es de tipo informático, como la difusión de mensajes injuriosos por medios informáticos o el fraude informático.

Además, ciertos países han adoptado textos especiales que combinan la regulación penal y otras de tipo administrativo, comercial, etc., una suerte de códigos temáticos sobre asuntos informáticos, por ejemplo, la ley sueca de 11 de mayo de 1973, parcialmente revisada en 1979; la ley alemana de protección de datos de enero de 1977; la Privacy Act de los Estados Unidos de diciembre de 1974; la ley No. 675 en Italia, sobre tutela de las personas y otros sujetos respecto al tratamiento de datos personales; y la ley francesa sobre informática y libertades de 1978, entre otros. En nuestro ámbito regional es de destacar la ley argentina 24.769 relativa a fraudes fiscales y previsionales; el Código Penal del Paraguay de 1998 que contiene dos tipos específicos: los arts. 174, "Alteración de Datos" y 175 "Sabotaje de computadoras"; y la Copyright Modernization Act canadiense de 2012.

3. ¿Qué es un delito informático o un cibercrimen?

En líneas anteriores hice alusión a las oportunidades delictivas que ofrecen las nuevas tecnologías de la información y la comunicación y, en especial, Internet. Se trata, por una parte, de su explotación como instrumento para la comisión de delitos que también podrían ser perpetrados por otros medios, una estafa, por ejemplo y, por otra parte, de actos que comprometen la integridad, accesibilidad o disponibilidad de la información que se encuentra en la red o los derechos del titular de un elemento informático, como el *hacking*, por ejemplo.

Dice Miró Llinares:

> "En los estudios criminológicos y jurídicos llevados a cabo en inglés, ya parece haberse impuesto este término [cybercrime] frente a otros que ocupan generalmente el mismo o similar espacio de significado, tales como computercrime y otros en los que se utilizan prefijos como virtual, online, high-tech, digital, computer-related, Internet-related, electronic, y e-crimes. En la raíz de este cambio de denominación está, a mi parecer, la mayor capacidad del término cibercrimen para expresar la característica esencial que une a esta forma de criminalidad y que la diferencia de otro tipo de delincuencia. Me refiero a que la primera se realiza en un nuevo ámbito o espacio con características estructurales intrínsecas y extrínsecas tan distintas a las del espacio físico en el que se ejecuta la delincuencia tradicional, que obliga a una revisión criminológica de la explicación del evento delictivo, así como una adaptación de las normas jurídicas para su mejor prevención" (Miró Llinares, 2011, p. 3).

Aunque al momento no se ha logrado un consenso sobre el concepto de "cirbercriminalidad", se admite generalmente que el término hace referencia a un conjun-

to de actividades ilícitas cometidas mediante el uso (tal vez sería más apropiado decir abuso) de las tecnologías de la información y la comunicación. Entonces, para que se configure un delito de esta categoría se requiere la utilización de un elemento informático en la comisión del hecho punible o que el resultado de la acción consista en la vulneración de un sistema informático.

La idea original de que los delitos cometidos en el ámbito informático o por medios informáticos son un nuevo tipo de criminalidad dio paso a la idea de una multiplicidad de modalidades de ataque contra diversos intereses de naturaleza individual o colectiva, unas veces al amparo y otras contra sistemas que contienen datos de personas naturales o jurídicas. Hasta fines de los ochenta, el núcleo de la conducta en estos nuevos delitos se centraba en los ataques a la privacidad. A medida que el acceso a tales sistemas se volvió masivo, los verbos rectores se expandieron a contenidos como "ataques", "fraudes", "espionaje", "destrucción" o "alteración" de los sistemas informáticos y/o los datos contenidos en ellos. Luego, con la apertura de Internet (que en realidad existía desde la década de los 70, pero pensado en un primer momento como una plataforma con posibles aplicaciones militares y no para el acceso público) y con el abaratamiento y consecuente acceso masivo de la población general a software de sistemas operativos, aplicaciones de productividad, música y videos en formato digital, el foco de atención penal en este ámbito pasó a ser la propiedad intelectual de los autores de los programas y otros componentes o productos informáticos, principalmente por la proliferación de copias ilegales de los mismos. Al tiempo, empezó a prestarse atención a ciertos contenidos que podrían afectar los derechos de determinados grupos de población, como la pornografía infantil, la promoción de la violencia xenófoba o las estructuras de inversión piramidal y *scams* económicos. En el último tiempo, la preocupación principal en esta materia se ha centrado en la seguridad de los servicios y plataformas de Internet, particularmente en aquellos utilizados por entidades públicas, bajo un supuesto riesgo permanente de actos de terrorismo informático[9].

Los delitos que nos ocupan ya no se ejecutan desde ordenadores, sino a través de las redes a las que están conectados, en un ámbito de comunicación universal, en el Ciberespacio y, precisamente, por la naturaleza de ese espacio virtual accesible desde cualquier espacio físico localizado en cualquier país del mundo, las infracciones que se cometen de esta manera pueden afectar, en lugares distintos y de manera simultánea bienes jurídicos muy diversos, pertenecientes a individuos o colectivos también diversos. Lo anterior plantea desafíos de la más variada naturaleza para la persecución y sanción de estos delitos, como examinaremos en un apartado posterior.

---

9 Para ahondar en esta cuestión se puede ver, Sieber, Ulrich, El control de la complejidad en el Ciberespacio global: La armonización de los delitos informáticos, en Delmas-Marty, Mireille; Pieth, Mark; y otros (directores) y Morales, Marta (coordinadora), Los caminos de la armonización penal (Valencia, Tirant Lo Blanch, 2009), pp. 158-161.

4. ¿Qué pretendemos proteger? (bienes jurídicos protegidos a través de las figuras penales de los cibercrímenes)

En el derecho penal se utiliza el término "bien jurídico" para identificar aquellos objetos que merecen una protección jurídico penal. Tales objetos pueden ser valores trascendentes para un determinado grupo social, objetos en el sentido ordinario del término, intereses individuales o colectivos, situaciones propias de la convivencia social o las condiciones de estas, etc. El concepto es tan vasto que hasta ahora es imposible que la doctrina penal se ponga de acuerdo para adoptar una definición absoluta de bien jurídico protegido que nos indique qué pretendemos salvaguardar mediante la intervención estatal en uso de su potestad punitiva.

Sin embargo, en general, como afirman Bustos y Hormazábal: "[l]os objetos de protección, los bienes jurídicos, surgen de la base social y, por consiguiente, están también sujetos a su rediscusión democrática. Por eso, se dice que tienen un carácter dinámico" (Bustos y Hormazábal, 1997 p. 57).

Ahora bien, para tratar de identificar esos objetos que merecen la protección del derecho penal vale la pena plantearnos esta pregunta de Rodotà: "¿qué significa vivir continuamente en público, en una dimensión que cancela las fronteras entre la esfera pública y privada, en un flujo continuo de informaciones que cambian la noción misma de identidad?" (Piñar Mañas, 2011, p.37).

Tomando en cuenta la definición de cibercrímenes ensayada en el apartado precedente podríamos sostener que los bienes jurídicos que se busca cautelar a partir de estas figuras penales son, en efecto, objetos novedosos, empezando por el propio Ciberespacio[10], entendido como el espacio virtual (no físico) de interrelación humana; la integridad de las plataformas y servicios informáticos; su seguridad; su disponibilidad; su accesibilidad; y los datos almacenados en tales plataformas.

Al tiempo, los denominados cibercrímenes permiten tutelar bienes jurídicos tradicionales como la vida privada; la honra y dignidad; la integridad y libertad sexual; el patrimonio; la seguridad jurídica; y la buena administración pública.

El propósito es, para ambos tipos de bienes jurídicos (nuevos y tradicionales), evitar conductas lesivas que provienen de la actividad humana en y a través de Internet.

En todo caso, la selección de los objetos que merecen protección penal en esta materia,

> "[…] está condicionada en un Estado social y democrático de derecho por el respeto de la libertad y dignidad de las personas y de sus necesida-

10 El término fue acuñado en la literatura de ciencia ficción, específicamente en la novela *Neuromancer*, publicada por William Gibson en 1984, donde se describe como un espacio de alucinación consensual.

des. Esto significa que de ningún modo por encima del individuo puede haber otros intereses de grupo o de conservación o funcionamiento del sistema social" (Bustos y Hormazábal, 1997 p. 59).

5. Los cibercrímenes en el Código Orgánico Integral Penal

La legislación penal, que nos rige desde el 10 de agosto de 2014, llegó con el anunciado propósito de modernizar un sistema caduco. La propia exposición de motivos del Código Orgánico Integral Penal (COIP) propone adecuar "la legislación ecuatoriana a los nuevos desarrollos conceptuales que se han producido en el mundo y en la región, como mecanismo para asegurar un correcto funcionamiento de la justicia penal".

En la práctica, no obstante, nuestra nueva legislación penal es más de lo mismo que habitualmente tuvimos: "las normas sustantivas, procesales y ejecutivas penales vigentes no responden a una sola línea de pensamiento. Sus contextos históricos son muy diversos. Las finalidades y estructuras son distintas, sin coordinación alguna, inclusive contienen normas contradictorias. Esto se traduce en un sistema penal incoherente, poco práctico y disperso". Este lenguaje crítico no me pertenece, corresponde a la propia exposición de motivos del COIP que, en forma rimbombante, anunciaba el final de los anacronismos y dispersiones normativos, para dar paso a la armonía y al vanguardismo penal, pero si tal era el propósito, entonces los legisladores debieron empezar por no copiar textualmente muchas disposiciones de nuestro anterior Código Penal vigente desde 1938 y reparar un poquito más en la técnica legislativa para construir los nuevos tipos penales.

En todo caso, lo que el legislador ecuatoriano ha hecho frente al fenómeno de la cibercriminalidad es identificar ciertas conductas que podrían cometerse empleando medios informáticos y solo excepcionalmente se ha ocupado de tutelar directamente la integridad, disponibilidad y/o accesibilidad de los sistemas informáticos y los datos alojados en ellos. También resulta notable que solo en un tipo penal se hace una alusión directa al Internet.

A continuación, examinaremos los tipos penales incluidos en el COIP que pueden ser categorizados como cibercrímenes por aludir de manera expresa, como bienes jurídicos protegidos o como instrumentos de comisión, a los sistemas y datos informáticos. Esto sin perjuicio de otros tipos penales en los que por la naturaleza de la conducta prohibida resultaría plausible el uso de Internet u otro mecanismo informático como instrumento.

a. Pornografía infantil

La Convención sobre los Derechos del Niño de 1989 dispone en su artículo 19 que "los Estados Partes adoptarán todas las medidas legislativas, administrativas, sociales y educativas apropiadas para proteger al niño contra toda forma de perjuicio o abuso físico o mental, descuido o trato negligente, malos tratos o explotación,

incluido el abuso sexual, mientras el niño se encuentre bajo la custodia de los padres, de un representante legal o de cualquier otra persona que lo tenga a su cargo". En cumplimiento de sus obligaciones internacionales, el Ecuador y los demás Estados del mundo están comprometidos desde hace décadas con el combate a la pornografía infantil.

Ahora bien, la pornografía infantil ha existido siempre, no es un fenómeno nuevo, sin embargo, es indiscutible que el Internet y, en particular, las redes sociales han asegurado el auge de este fenómeno. Antes esta conducta se caracterizaba por su marginalidad y clandestinidad, pero el Ciberespacio al favorecer el anonimato y dificultar la persecución del hecho ha promovido un notable incremento en la frecuencia con que se produce y divulga material pornográfico que muestra a niños o adolescentes. Por eso precisamente era indispensable, al actualizar nuestra legislación penal, incluir de manera expresa la mención a los medios informáticos como instrumento para la comisión del delito de pornografía infantil.

El enunciado general del artículo 103 del COIP establece:

> Art. 103.- Pornografía con utilización de niñas, niños o adolescentes.- La persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual; será sancionada con pena privativa de libertad de trece a dieciséis años.

Los bienes jurídicos protegidos en este caso no son solo la libertad e integridad sexual como en otros delitos sexuales, sino también, por la especial consideración al sujeto pasivo de la infracción, el normal desarrollo de la personalidad del niño o adolescente.

En general, la norma es clara respecto de cuáles son las modalidades de comisión del delito, sin embargo, entre los verbos rectores del tipo se encuentra "producir" que suponemos debería entenderse como la realización o financiamiento de las fotografías, videos o soporte de que se trate.

Si bien la pena contemplada para esta conducta no corresponde al nivel más elevado de las sanciones penales en nuestro ordenamiento, es claro que el legislador ha tomado la decisión consciente de atribuir a este delito una pena severa. Recordemos, en este sentido, que el propósito del declarado ordenamiento penal ecuatoriano (artículo 52 del COIP) es la prevención general, es decir, la disuasión del colectivo social de la comisión de delitos, mediante la advertencia de la gravedad de la sanción.

b.Violación de la intimidad

En vista de la tutela constitucional del derecho a la intimidad y confidencialidad de las comunicaciones, el legislador ecuatoriano ha resuelto castigar toda acción que implique un acceso o una divulgación no consentida de información privada por cualquier medio.

El artículo 178 del COIP determina lo siguiente:

> Art. 178.- Violación a la intimidad.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.
>
> No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley.

El objeto sobre el cual recaería la acción delictiva es múltiple. Consiste en soportes físicos o virtuales que recogen, incorporan o reproducen hechos, datos, expresiones de voluntad, etc., que constituyan secreto para alguien y afecten su intimidad o que, sin ser secreto, involucren dicha intimidad, como las fotografías publicadas en una red social accesibles solo para los amigos del sujeto pasivo. Además, la norma contiene una alusión directa a la información privada contenida en soportes informáticos como objeto de protección, más allá de la intimidad como bien jurídico tutelado de manera principal.

Como ocurre con el delito analizado en el apartado precedente, en este caso también las modalidades comisivas son varias, incluida la posible divulgación por medios informáticos.

Es importante resaltar que bajo nuestro ordenamiento jurídico vigente, en todo caso, la existencia de una orden judicial podría justificar una invasión a la privacidad incluida la privacidad (al menos presunta) en red, lo que desde el punto de vista de los estándares internacionales de protección de los derechos humanos es por lo menos cuestionable.

Finalmente, vale recordar que la protección de la honra y la reputación, cuando su afectación se concreta mediante el uso de Internet, debe responder, en general, a criterios de ponderación similares a los que se utilizan en otros ámbitos de la comunicación. Pero desde luego, esto no tiene que ver con la construcción del tipo penal, sino con la interpretación que el funcionario llamado a aplicarlo realice del mismo.

c. Fraudes cibernéticos

El fraude cibernético es el delito informático por antonomasia, probablemente por su simplicidad que no exige conocimientos informáticos demasiado sofisticados y por el notable rédito económico que puede generar.

Se denomina ciberfraude o fraude cibernético a las conductas en las que los sistemas informáticos se convierten en instrumento para lograr un beneficio patrimonial ilícito derivado de un perjuicio patrimonial a una víctima.

Estas conductas pueden adoptar diversas modalidades que van desde el simple envío de correos *scam*, para conseguir que el sujeto pasivo entregue información personal que facilite el acceso a sus cuentas, hasta la intrusión en los complejos sistemas informáticos de entidades financieras para conseguir la transferencia involuntaria de determinados activos, pasando por la introducción de datos falsos, la alteración de los programas o la utilización de bombas lógicas y virus que provocan la realización automática de transferencias bancarias, ingresos o reconocimiento de créditos en favor de quien realiza la alteración.

La característica principal de los fraudes es la puesta en escena, el engaño al sujeto pasivo que le induzca al error para que se produzca, en consecuencia, el acto de disposición patrimonial. Pero tratándose de un fraude cibernético, en realidad no se produce el engaño, sino, en todo caso, la falta de una debida diligencia de la supuesta víctima o de un tercero en el cumplimiento de su deber de comprobación de la identidad de la supuesta contraparte en la transacción de que se trate o alternativamente la afectación del patrimonio ajeno sin conocimiento de la víctima ni del responsable de la administración de su patrimonio, de manera automática y sin ningún contacto personal. El elemento del engaño, entonces, es sustituido por la manipulación informática.

Por eso, frente a este tipo de comportamientos, los tipos tradicionales de estafa no son respuestas apropiadas, dado que en ellos el apoderamiento del dinero o bienes ajenos se produce en un sentido físico o material que no se da en la mayor parte de estas conductas en las que, además, hay muchos casos en los que la propia víctima es quien ejecuta el acto de disposición patrimonial que la perjudica.

Entonces resulta necesaria una tipificación específica. En el caso de la legislación penal ecuatoriana se identifican dos formas de ciberfraude:

Por una parte, el artículo 190 del Código Orgánico Integral Penal señala lo siguiente:

> Art. 190.- Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamien-

> to de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.
>
> La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.

Y, por otra, el artículo 231 dispone:

> Art. 231.- Transferencia electrónica de activo patrimonial.- La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.
>
> Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.

En ambos tipos el objetivo perseguido por el legislador parece ser la protección del patrimonio frente al uso de sistemas electrónicos o informáticos, que es lo que se describe como comportamiento típico.

d. Falsificaciones cibernéticas

Lo característico de estos delitos es la alteración de datos o información contenida en documentos almacenados en sistemas informáticos.

La necesidad de una tutela penal de los datos o información contenida en documentos almacenados en sistemas informáticos tiene que ver con que los documentos digitales desempeñan una función cada vez más importante, se utilizan con mayor frecuencia. La utilización de documentos digitales, en sustitución de documentos físicos, se sustenta por medios jurídicos como, por ejemplo, la legislación que reconoce las firmas electrónicas.

Nuestra legislación penal vigente contempla dos tipos de falsificación cibernética en particular:

El artículo 211 del COIP contempla un supuesto de falsificación de los datos de registro civil de una persona.

> Art. 211.- Supresión, alteración o suposición de la identidad y estado civil.- La persona que ilegalmente impida, altere, añada o suprima la

> inscripción de los datos de identidad suyos o de otra persona en programas informáticos, partidas, tarjetas índices, cédulas o en cualquier otro documento emitido por la Dirección General de Registro Civil, Identificación y de Cedulación o sus dependencias o, inscriba como propia, en la Dirección General de Registro Civil, Identificación y de Cedulación a una persona que no es su hijo, será sancionada con pena privativa de libertad de uno a tres años.

Debe notarse que la alteración de registros electrónicos es una entre varias modalidades comisivas de este delito y que la finalidad específica perseguida con la alteración de la información de registro civil resulta intrascendente.

En el artículo 298, numerales del 8 al 10 del COIP, la conducta prohibida consiste en la falsificación de datos informáticos con el propósito de evadir el pago de impuestos.

La norma en cuestión establece lo siguiente:

> Art. 298.- Defraudación tributaria.- La persona que simule, oculte, omita, falsee o engañe en la determinación de la obligación tributaria, para dejar de pagar en todo o en parte los tributos realmente debidos, en provecho propio o de un tercero, será sancionada cuando:
>
> [...]

8. Altere libros o registros informáticos de contabilidad, anotaciones, asientos u operaciones relativas a la actividad económica, así como el registro contable de cuentas, nombres, cantidades o datos falsos.

9. Lleve doble contabilidad con distintos asientos en libros o registros informáticos, para el mismo negocio o actividad económica.

10. Destruya total o parcialmente, los libros o registros informáticos de contabilidad u otros exigidos por las normas tributarias o los documentos que los respalden, para evadir el pago o disminuir el valor de obligaciones tributarias.

> [...]
>
> Las penas aplicables al delito de defraudación son:
>
> En los casos de los numerales del 1 al 11, será sancionada con pena privativa de libertad de uno a tres años.

Los supuestos descritos en los numerales 8 y 10 corresponden a escenarios de falsedad material, mientras que el supuesto descrito en el numeral 9 corresponde a escenarios de falsedad ideológica.

e. Delitos contra la confidencialidad, accesibilidad, integridad y disponibilidad de datos y sistemas informáticos

El legislador ecuatoriano también se preocupó, al actualizar la normativa penal, de incluir en el catálogo de delitos una serie de conductas que atentan contra la confidencialidad, accesibilidad, integridad y disponibilidad de datos y sistemas informáticos.

i. Estos son los cibercrímenes stricto sensu, es decir, aquellos en los que el bien jurídico protegido son propiamente los datos y sistemas informáticos: Revelación ilegal de bases de datos

El artículo 229 del COIP determina que:

> La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.
>
> Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

Los criterios explicados dentro del análisis del delito de violación de la intimidad en el apartado "b" de la presente sección, son también aplicables a este tipo penal.

Cabe simplemente agregar que en su segundo inciso el tipo[11] presenta una modalidad agravada en atención a una condición personal del sujeto activo (ser servidor público o empleado de una institución financiera), aparentemente con el propósito de tutelar el patrimonio de las personas más allá de su intimidad o privacidad.

ii. Interceptación ilegal de datos

La única disposición del Código Orgánico Integral Penal que contiene una referencia expresa al Internet es el artículo 230 que castiga la intercepción ilegal de datos en los siguientes términos:

11 Tipo es la descripción que contiene la ley de la conducta prohibida y de la consecuencia jurídica de incurrir en ella.

Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.

2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de Internet diferente a la que quiere acceder.

3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.

4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

Contra lo que se pudiera pensar: este tipo penal no pretende tutelar únicamente la privacidad de las personas, del lenguaje empleado en su redacción se desprende que la norma también protege el patrimonio y, en general, los datos informáticos aun si no tienen la característica de secretos.

En este caso, los móviles de los delincuentes pueden ser muy diversos. Algunos simplemente quieren burlar las medidas de seguridad para probar sus propias capacidades, otros actúan por motivos políticos.

iii. Ataque a la integridad de sistemas informáticos

En el artículo 232 del COIP el legislador pretende castigar conductas como borrar, suprimir o modificar sin autorización funciones o datos informáticos con intención de obstaculizar el normal funcionamiento del sistema. Se trata del delito tradicionalmente conocido como sabotaje cibernético.

La norma en cuestión señala:

> Art. 232.- Ataque a la integridad de sistemas informáticos.- La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.

2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.

La comisión de estos delitos exige conocimientos especializados de programación para la destrucción o modificación de datos, sea mediante bombas lógicas que se insertan en el sistema para provocar una alteración futura, gusanos que se infiltran en programas legítimos para modificar o destruir los datos contenidos en determinado sistema (este tipo de programa dañino no puede regenerarse) o virus, es decir, programas dañinos que se reproducen a través del sistema y se contagian a otros sistemas con el propósito de destruir datos.

Una de las formas más comunes del sabotaje cibernético es la denegación distribuida de servicio (DDoS) que implica la inundación de un sistema informático con un volumen masivo de información para que el sistema se ralentice, casi hasta su inutilidad. Las denominadas *botnets* son el método preferido de los ciberdelincuentes, ya que realizan múltiples solicitudes de servicio coordinadas.

iv. Obtención de información pública reservada

El artículo 233 del COIP sanciona a:

> La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años.

El segundo inciso de la norma en cuestión castiga a:

> La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años.

Es únicamente esta segunda conducta descrita en la norma la que puede ser catalogada como cibercrimen. Es importante destacar que nos encontramos frente a uno de esos delitos que la doctrina denomina especiales, es decir, en los que entre los elementos del tipo se encuentra la exigencia de un sujeto activo calificado, un servidor público. Sin embargo, en la práctica, el acceso y la obtención de la

información reservada bien pudieran ser ejecutados por cualquier *hacker* o pirata cibernético.

Internet se utiliza cada vez más para obtener secretos. El valor de la información confidencial y la capacidad de acceder a la misma a la distancia hacen que el espionaje de datos resulte tentador para los ciberdelincuentes quienes se valen de mecanismos como: software para explorar los puertos desprotegidos o software para burlar las medidas de protección, inclusive complejos sistemas de cifrado.

En el siguiente apartado ahondaré en las particularidades de los accesos no autorizados o no consentidos a los sistemas informáticos.

v. Acceso no consentido a sistemas informáticos

La piratería cibernética es castigada por el COIP en estos términos:

> Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.

El acceso no consentido se efectúa ordinariamente desde un lugar exterior, situado en la misma red, aprovechando la deficiencia o ausencia de medidas de seguridad para obtener acceso. A menudo, se hacen pasar por usuarios legítimos del sistema y utilizan claves de acceso clonadas o programas que permiten automatizar los ataques con lo que un solo pirata puede afectar miles de terminales en un solo día.

En la mayoría de estos casos, el móvil no se limita al acceso ilícito del sistema informático, sino que este es un medio para perpetrar otros delitos, como el espionaje o la manipulación de datos y los ataques de denegación del servicio.

En los últimos años, los delincuentes han concentrado sus ataques en los computadores privados, muchos de los cuales no están adecuadamente protegidos. Además, los computadores privados suelen contener información delicada (por ejemplo, datos bancarios o de tarjetas de crédito). Otra razón por la que atacan a los computadores privados es que, si el ataque resulta satisfactorio, los delincuentes pueden incluir dicho computador en su red zombi y, por ende, utilizarlo para otras actividades delictivas.

Lo que parece problemático en el tipo penal del artículo 234 del COIP es que confunde el acceso ilícito con delitos que pueden cometerse después como "modificar un portal web, desviar o redireccionar de tráfico de datos o voz".

6. *Problemas en la persecución penal de los cibercrímenes*

Había advertido líneas atrás sobre los desafíos que plantea la persecución penal en cuanto a las conductas perpetradas en y a través de Internet que dañan o ponen en riesgo determinados bienes jurídicos.

Entre otros problemas que presentan los cibercrímenes en términos sustantivos y procesales penales tenemos que: se cometen a distancia; con la inigualable protección para el sujeto activo que otorga el anonimato; sin posibilidad de una reacción inmediata del sujeto pasivo en defensa de sus bienes jurídicos afectados, en general, se trata de delitos instantáneos, es decir, de aquellos en que los momentos de comisión y consumación coinciden; podrían motivar problemas de jurisdicción aplicable tomando en consideración la diversa ubicación geográfica de los sujetos activos y pasivos, así como de los proveedores de servicios o contenidos cuyas plataformas fueron aprovechadas como instrumento de la infracción; pueden afectar a través de una sola acción criminal a múltiples víctimas y preservar su potencialidad multiplicadora a través del tiempo; por la actual facilidad y universalidad en el acceso a la red, los sujetos activos del hecho pudieran ser personas inimputables, especialmente, menores de edad, etc.

Sin pretender ser exhaustivo, a continuación, analizaré brevemente algunos de los aspectos más complejos del tratamiento penal de los cibercrímenes y los criterios desarrollados en el derecho comparado e internacional para superarlos.

a. ¿Quién es responsable?

La actividad en Internet involucra a diferentes actores (usuarios, proveedores de servicios, proveedores de contenidos y otros). El usuario es la persona física o jurídica que mantiene una página, el titular y el encargado de la página. El proveedor de servicios es la empresa que se dedica a conectar a los usuarios individuales a la red, a cambio de un precio o canon, generalmente mensual. Por último, el proveedor de alojamiento o de contenidos es la empresa que destina parte de su plataforma o espacio virtual para alojar la página de una persona. El proveedor de acceso, en la mayoría de los casos, tiene ubicación en el mismo lugar que el usuario, pero quien brinda el alojamiento puede estar en cualquier lugar del mundo.

La circulación de informaciones e ideas en Internet no sería posible sin estos actores, al tiempo, esta diversidad de actores y también la diversidad de ubicaciones, como veremos más adelante, generan graves problemas al momento de determinar los responsables de un eventual ilícito.

Por eso, hace ya algún tiempo, los Estados vienen diseñando fórmulas para que los intermediarios en Internet respondan por los posibles delitos cometidos por sus usuarios. En efecto, como observa Cortés:

> "En muchas ocasiones es más fácil para el regulador influir en la conducta del individuo a través de esos terceros que de manera directa. Así,

le resulta más fácil al Estado que la aerolínea verifique si tenemos una visa vigente o que el banco cobre un impuesto por el dinero que enviamos al extranjero. Esta estrategia es conocida como teoría de intermediarios, amas de llaves o guardianes" (Cortés, 2014, p. 63).

En ciertos países, la presión de los propios actores privados (titulares de los derechos de autor, por ejemplo) para la atribución de responsabilidad penal a los intermediarios derivó, efectivamente, en la adopción de una legislación específica con tal propósito, la más notable es la *Digital Millennium Copyright Act* de Estados Unidos, sancionada en 1998[12].

En su informe al Consejo de Derechos Humanos de las Naciones Unidas de mayo de 2016[13], el Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión afirma:

> La función que desempeña el sector privado en la era digital parece estar generalizada y ampliarse constantemente, de manera que ese sector se ha convertido en uno de los elementos impulsores de la mayor expansión del acceso a la información de la historia. Algunos de los grandes foros de expresión pública de las redes sociales son propiedad de empresas privadas. Las principales plataformas que agregan e indexan el conocimiento global y diseñan los algoritmos que determinan qué información se publica en Internet son fruto de la iniciativa privada. Además, tanto la inversión en la infraestructura para la tecnología móvil, con la que miles de millones de personas se comunican y acceden a Internet, como su mantenimiento y titularidad están en manos privadas. Las herramientas que emplean las fuerzas del orden y los organismos de inteligencia se crean, por lo general, a partir de productos de los sectores privados de la vigilancia y el procesamiento de datos. Son empresas privadas las que diseñan, fabrican y generalmente mantienen los dispositivos o servicios donde se almacenan los datos personales más importantes (desde información financiera y sanitaria hasta correos electrónicos, mensajes de texto, historiales de búsqueda, fotografías y vídeos).

¿Deberían tener esos agentes privados las mismas responsabilidades que las autoridades públicas? ¿Deberían tales responsabilidades derivarse del derecho de los derechos humanos, de las condiciones de servicio, de los arreglos contractuales o de otras fuentes? ¿Cómo deberían estructurarse las relaciones entre las empresas y los Estados? Cuando se enfrentan con presiones para dirigir sus negocios de una manera que atente contra la libertad de expresión, ¿qué medidas deben adoptar los agentes privados? ¿Negarse a entrar en los mercados o salir de ellos? ¿Aconsejar a sus clientes sobre esas presiones? A medida que el mundo se adentra

---

12 http://www.copyright.gov/legislation/dmca.pdf.

13https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/095/15/PDF/G1609515.pdf?OpenElement.

cada vez más en el espacio digital, con la "Internet de las cosas" en un horizonte próximo, es esencial ofrecer pautas sobre cómo garantizar la promoción, la protección y el disfrute de los derechos.

Por su parte, la Declaración Conjunta sobre Mecanismos Internacionales para la Promoción de la Libertad de Expresión suscrita el 21 de diciembre de 2005, por los relatores para la libertad de expresión de las Naciones Unidas, la Organización para la Seguridad y Cooperación en Europa y la OEA, claramente señala que "[l]as personas no deben ser consideradas responsables por el contenido de Internet que no es de su autoría, a menos que hayan adoptado el contenido como propio o se hayan negado a obedecer una orden de un tribunal para remover ese contenido".

En todo caso, si de manera excepcional, la legislación de un Estado permitiera la atribución de responsabilidad a los intermediarios, en lugar de los usuarios, es necesario tomar en cuenta que, por su naturaleza, los cibercrímenes, en general, son dolosos, no culposos y, por lo tanto, el intermediario del que se trate debería encontrarse en posición de garante de los bienes jurídicos afectados y haber omitido, de manera grave, su obligación de garantizarlos.

Sin embargo, precisamente para evitar consecuencias severas, como son las penales, los intermediarios han optado por colaborar con los Estados en tareas de vigilancia y censura de contenidos o control del tráfico en Internet, acciones que terminan por violar los derechos de los usuarios.

Así, los Estados ordinariamente solicitan a los intermediarios que retiren contenido aduciendo motivos de difamación, blasfemia, normas electorales, acoso o discurso de odio, provocación, propiedad intelectual, obscenidad e indecencia, captación para actividades terroristas o enaltecimiento del terrorismo, protección de la seguridad nacional y la seguridad pública, protección de la infancia y prevención de agresiones sexistas.

Los Estados también han regulado algunos problemas asociados a la libertad de expresión que existen desde hace mucho tiempo, pero que se complican cada vez más en la era digital, como el "derecho al olvido" y la pluralidad y la diversidad (por ejemplo, la neutralidad de la red). Los intermediarios, por su parte, establecen y aplican unas condiciones de servicio diseñadas para otorgarles impunidad en esta tarea policiva. La censura privada se complica por la gran cantidad de denuncias y de contenido sospechoso que los intermediarios identifican diariamente. Las plataformas de mayor tamaño también pueden subcontratar la gestión del contenido, lo que a su vez deja en manos de terceros, no vinculados a los proveedores, la posibilidad de decidir qué es bueno y qué es malo.

De cualquier forma, el control directo sobre los posibles autores de los contenidos ilícitos, por parte de los intermediarios o sus gestores, parece casi imposible de realizar, tanto por el anonimato (que examinaremos más adelante), como por la movilidad de los delincuentes.

b. Tiempo y espacio

Los sistemas penales tradicionales están diseñados para operar dentro de un marco territorial específico que está sujeto a la soberanía de un Estado particular. Al no existir fronteras reales en Internet, es difícil decidir cuál es la jurisdicción aplicable o prevalente frente a la comisión de delitos en o valiéndose de dicho espacio tecnológico.

Al tiempo, esa dispersión geográfica puede provocar que un uso ilícito de Internet, que ya fue materia de investigación o sanción, sea nuevamente juzgado por otro Estado, violándose, de esta manera, la prohibición de doble juzgamiento, uno de los pilares del derecho penal moderno.

Y por si fuera poco, también es posible que un contenido ilícito en Internet por el cual ya se atribuyeron responsabilidades penales sea luego replicado en una segunda, tercera o enésima ocasión, lo que plantea la interrogante de si pueden esas reiteraciones del delito ser o no castigadas.

Ahora bien, no se trata de que Internet no esté en ningún sitio o de que esté en todos. La realidad es que materialmente la información que circula en Internet está alojada en servidores distribuidos en lugares específicos alrededor del mundo, discos duros conectados entre sí y con la red, sujetos a sofisticadísimas medidas de seguridad, precisamente por la sensibilidad de los datos que contienen. La dificultad, en realidad, radica en encontrar el lugar donde está depositada determinada información de Internet, tomando en cuenta el secretismo con que se maneja la localización de los centros de datos, lo que, sin embargo, será determinante al momento de atribuir responsabilidades por la comisión de delitos en o mediante la red.

La cuestión se complica aún más si los contenidos ilícitos son camuflados en cuanto a su origen, a través de la utilización de *mirrors*, de manera que una página de Internet puede, en realidad, estar en un lugar diferente al que aparenta.

Sobre esta cuestión, la Declaración Conjunta sobre Mecanismos Internacionales para la Promoción de la Libertad de Expresión suscrita el 21 de diciembre de 2005 por los relatores para la libertad de expresión de las Naciones Unidas y la Organización para la Seguridad y Cooperación en Europa y la OEA, establecen que: "[l]a jurisdicción en casos relativos a Internet debe restringirse a aquellos Estados en los que el autor se haya establecido o a los cuales el contenido se haya dirigido específicamente; no debe establecerse la jurisdicción en un Estado simplemente porque el contenido haya sido descargado allí"[14].

Asimismo, la relatoría especial para la libertad de expresión de la OEA ha destacado la importancia de "que las autoridades adopten reglas jurisdiccionales com-

14 Declaración Conjunta sobre Mecanismos Internacionales para la Promoción de la Libertad de Expresión suscrita el 21 de diciembre de 2005, disponible en: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=650&lID=2

patibles con la noción de publicación única que previene tanto el efecto indeseable de la selección deliberada de una jurisdicción (*forum shopping*) como el doble juzgamiento por una misma causa (*non bis in idem*)"[15].

Frente a contenidos publicados "[…] con el mismo formato y en el mismo lugar, los plazos para la interposición de acciones judiciales deberían computarse desde la primera vez que fueron publicados […]" y se debe garantizar que no pueda promoverse más de una acción por los daños causados por tales contenidos y otorgarse "[…] una única reparación por los daños sufridos en todas las jurisdicciones (regla de la "publicación única")"[16].

En este sentido, es importante mencionar que, si bien la cooperación internacional ha avanzado en materia de asistencia judicial y policial a través de medidas que permiten la colaboración en la obtención de fuentes de prueba, el intercambio de información o la entrega de detenidos, en cambio, no ha avanzado mucho en la búsqueda de soluciones procesales destinadas a evitar los procedimientos penales paralelos. Por ende, la comunidad internacional debe avanzar en el desarrollo de criterios para la selección consensual de la jurisdicción penal más idónea en casos de litispendencia internacional y de estándares para el reconocimiento recíproco de las decisiones judiciales adoptadas en el espacio internacional acordado en los ámbitos penal y procesal.

Por último, está el problema de los "paraísos tecnológicos", es decir, aquellos países donde no existen leyes que limitan estas conductas o que las tratan de modo más permisivo.

En suma, la prevención de los conflictos jurisdiccionales frente a la cibercriminalidad exige una armonización racional y consensuada de los criterios de determinación de los límites y criterios de la competencia nacional en las legislaciones de los Estados. Esto no equivale a renunciar a la propia soberanía sino, por el contrario, afirmarla, negociando con los pares pautas de actuación futura.

c. Nacionalidad del sujeto activo y del sujeto pasivo

Además de lo anterior, tomando en consideración que Internet es accesible desde cualquier lugar del mundo, en términos reales, un individuo puede cometer un delito contra otro ubicado a miles de kilómetros de distancia, utilizando servidores localizados en un tercer estado, inclusive sin saber dónde se halla su víctima.

---

15 CIDH. Informe sobre Libertad de Expresión e Internet, disponible en: http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_web.pdf

16 Declaración Conjunta sobre Libertad de Expresión e Internet. Firmada por el Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión, la Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Relatora Especial de la Organización de Estados Americanos (OEA) para la Libertad de Expresión y la Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP) el 1 de junio de 2011 punto 4 literal c).

Lo anterior ha motivado a que más allá de la localización de los soportes físicos de los sistemas informáticos, de los servidores y, por ende, de los datos o del lugar geográfico donde empieza a cometerse un delito cibernético y de aquel en que ha de producir sus efectos, los Estados empiecen a reclamar para sí la jurisdicción penal para castigar tales conductas a partir de criterios de personalidad activa o pasiva.

En efecto, ciertos estados pretenden afirmar su jurisdicción tomando en cuenta que la víctima es su nacional (personalidad pasiva) o que el autor del hecho es su nacional (personalidad activa). Esto genera también conflictos jurisdiccionales.

d. Defensa de intereses locales

También podría ocurrir que un Estado reclame para sí la jurisdicción frente a determinado cibercrimen, no por la nacionalidad del sujeto activo o pasivo, sino por la nacionalidad del bien jurídico afectado, causando un nuevo conflicto jurisdiccional con los Estados que pretendan investigar el hecho basados en los principios de territorialidad o personalidad.

e. Anonimato

En estricto sentido, no existe anonimato en Internet. Esto porque todo terminal conectado a la red cuenta con una identificación única que permite individualizarlo: la dirección IP.

Además, hay programas diseñados para detectar y mantener registros de la historia de navegación en línea, tanto de las rutas que hemos seguido, como de los dispositivos (computadores, teléfonos inteligentes, *tablets*, etc.), aplicaciones, herramientas y protocolos que hemos empleado.

También el usuario va dejando una suerte de huellas digitales a medida que "acepta" las denominadas *cookies*, que facilitan su localización y que, de hecho, son parte del estímulo para las empresas que se dedican a proveer servicios o contenidos; al capturar información del usuario localizan potenciales clientes, de ahí el usual bombardeo de publicidad cuasi personalizada que normalmente reciben los usuarios de Internet.

Toda esa información, combinada con la dirección IP y otros datos alojados en las plataformas de los proveedores de servicios y contenidos, pueden ayudar a individualizar a algún usuario en particular.

Sin embargo, aun logrando la individualización del usuario, todavía nos quedaría pendiente lograr su identificación y, por supuesto, los delincuentes que operan en Internet están habituados a adoptar una serie de medidas tendientes a impedir justamente su identificación.

"De hecho, la relativa dificultad técnica para detectarlo se contradice con la casi inalcanzable validez procesal de la información así obtenida y/o la enorme complejidad legal de conseguir, a tiempo" (Velasco Núñez, 2010, p. 93).

Es esta percepción de seguridad con la que actúa el delincuente, ese temor mínimo a ser detectado y peor aún detenido, esa tranquilidad de actuar desde la comodidad de su casa, sin terceros que presencien el hecho, adoptando diversos nombres y personalidades falsas, lo que le resulta atractivo para emplear el Internet como instrumento para la perpetración de delitos o directamente como objetivo de su ataque.

De hecho, aunque parezca contradictorio, en el caso del sujeto activo de los cibercrímenes es también el percibido anonimato lo que le lleva a considerarse inmune a un eventual ataque a sus derechos. Por eso, la mayoría de cibernautas no adoptan medidas de seguridad mayores para preservar sus datos como ocultar su estatus económico o su patrimonio, impedir que otros usuarios accedan a su perfil en redes sociales o que puedan tener acceso a imágenes, videos y otros elementos de información muy privados. Es decir, la propia sensación de anonimato de la potencial víctima es un factor de riesgo para la comisión de estos delitos.

Al tiempo, sugerir limitaciones al anonimato para promover mayores niveles de seguridad para que la red pudiera comprometer los derechos de los usuarios: la libertad de expresión, la intimidad, la protección de datos y el secreto de las comunicaciones, entre otros. Podría, de hecho, considerarse cualquier medida implementada en tal sentido como una forma de censura o una acción contraria al principio de neutralidad de la red.

Sin perjuicio de lo anterior, la complejidad de implementar en la práctica reglas de restricción del anonimato sería altísima, pues implicaría que en todos los países del mundo se impida el acceso a Internet sin identificación y, seguramente, se volvería un negocio muy lucrativo justamente la provisión de mecanismos para "volverse invisible". Precisamente, en la actualidad, ya existen una serie de programas y aplicaciones cuya finalidad específica es preservar el "anonimato" en la red, como los sistemas de mensajería encriptada, el alquiler de direcciones electrónicas temporales, los programas de navegación sin rastro, etc.

f. Particularidades de la investigación

Por la naturaleza de los cibercrímenes, su detección e investigación no puede seguir los parámetros empleados para los delitos tradicionales. La recolección de evidencia para fundamentar una acusación y luego adelantar un juicio es, en estos casos, muy compleja, empezando por la identificación del sospechoso, pues como se explicó en el apartado precedente, es muy difícil llegar a conocer con precisión quién está detrás de la pantalla.

Si llegamos a identificar al sujeto activo, seguramente necesitaremos una autorización judicial para proceder a la intercepción de datos o vigilancia de la actividad en Internet o para aprehender los soportes físicos que contengan la evidencia del ilícito. En estas situaciones la oportunidad de la intervención es crucial, pues la prueba puede viciarse o simplemente perderse con gran simplicidad.

Por otra parte, es posible que la evidencia consista en datos cifrados, en cuyo caso además sería necesario un proceso de decodificación.

A lo anterior pudiera añadirse la falta de conocimiento del propio sujeto pasivo sobre la afectación de la que fue objeto con la consecuente demora en la presentación de una denuncia, o los resquemores a que ciertos aspectos de la vida privada sean expuestos como resultado de las investigaciones, o que la reputación del intermediario de Internet que puede corroborar el hecho se vea comprometida.

La duración legal de la obligación de conservar los datos varía de un país a otro, lo que también complica los procesos de investigación pues, en muchos casos, cuando finalmente se presenta un requerimiento formal, la evidencia ya fue desechada. Además, con fundamento en la reciente jurisprudencia internacional y local sobre el "derecho al olvido", el retiro de contenidos y la consecuente desaparición de posibles elementos relevantes para el esclarecimiento de un ciberdelito es mucho más simple.

Y desde luego, deberá contarse con peritos informáticos capaces de traducir a un lenguaje comprensible por los operadores de justicia las particulares complejidades técnicas de los cibercrímenes, lo que por ahora en Ecuador es uno de los mayores problemas, considerando que para actuar como experto judicialmente es indispensable contar con un registro ante el Consejo Nacional de la Judicatura, trámite burocrático engorroso que los académicos y profesionales destacados en diversos ámbitos prefieren no tener que sufrir. El resultado, entonces, es que los fiscales designan a cualquier persona con un conocimiento elemental, no especializado, con tal que tenga el respectivo registro.

7. *Evitando abusos: estándares internacionales sobre libertad de expresión*

Al adoptar decisiones de política criminal en materia de cibercriminalidad los Estados deben tomar en cuenta que una regulación inapropiada puede terminar por comprometer derechos constitucional e internacionalmente reconocidos, en particular la libertad de expresión; además, las previsiones mínimas deben ser implementadas para garantizar bienes jurídicos en riesgo a partir de usos inapropiados de las tecnologías de la comunicación e información, aun echando mano del carácter aflictivo del derecho penal y que por la naturaleza de las infracciones cometidas en y a través del Internet, sin duda serán necesarias para garantizar efectividad en la protección de los bienes jurídicos ya mencionados, tener la colaboración de otros gobiernos en la forma de apoyo técnico o judicial para una adecuada investigación y sanción de estos delitos.

Afortunadamente, como fue explicado en el apartado 2 del presente artículo, la comunidad internacional viene tomando previsiones en esta materia desde hace al menos tres décadas.

Para complementar lo ya dicho en materia de estándares sobre ciberseguridad y cooperación, me referiré a algunos de los aspectos más destacables de los estándares internacionales sobre libertad de expresión a ser considerados en el combate a la cibercriminalidad:

En razón que Internet es también un espacio (virtual desde luego), donde las personas ejercemos nuestros derechos, incluida la libertad de expresión, "la soberanía de los Estados ha encontrado en Internet un obstáculo: la libertad en la red se ha convertido en una manifestación decisiva de las libertades públicas, en una nueva expresión de las garantías de los ciudadanos" (Moles Plaza, 2004, p. 21).

En este sentido, como ha expresado hace pocos meses el Relator Especial de Naciones Unidas sobre Libertad de Expresión:

> En el mundo virtual, las personas disfrutan también de todos los demás derechos, como el derecho a la vida privada, a las creencias religiosas, el derecho de asociación y de reunión pacífica, el derecho a la educación, a la cultura y el derecho a no ser objeto de discriminación. Los Estados tienen tanto la obligación negativa de abstenerse de violar derechos como la positiva de garantizar su disfrute. Para cumplir esas obligaciones positivas, es probable que las autoridades públicas tengan que adoptar medidas para proteger a las personas de los actos de partes privadas[17].

Pero la garantía de los derechos de los ciudadanos por parte del Estado no implica una posibilidad ilimitada de restricción de esos mismos derechos para impedir su ejercicio abusivo. El Estado también se encuentra sometido a una obligación general de respeto de los derechos que implica una restricción en el ejercicio de su poder, a fin de no invadir ilegítimamente las esferas individuales[18].

En su informe sobre Libertad de Expresión e Internet del año 2013[19], publicado en 2014, la Comisión Interamericana de Derecho Humanos estableció:

> El entorno digital debe adecuarse a unos principios orientadores que informan la labor del Estado, el desarrollo de políticas públicas y la actuación de los particulares. Tales principios, que se explican brevemente en adelante, incluyen el acceso en igualdad de condiciones, el pluralismo, la no discriminación y la privacidad. En todo caso, es importante indicar que todas las medidas que puedan de una u otra manera afectar el acceso

17 Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, 11 de mayo de 2016, disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/095/15/PDF/G1609515.pdf?OpenElement, párr. 8.

18 Sobre esta cuestión puede verse: Corte I.D.H., *Caso Velásquez Rodríguez*. Sentencia de 29 de julio de 1988. Serie C No. 4.

19 CIDH. Informe sobre Libertad de Expresión e Internet, disponible en: http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_web.pdf.

> y uso de Internet deben interpretarse a la luz de la primacía del derecho a la libertad de expresión, sobre todo en lo que respecta a los discursos especialmente protegidos en los términos del artículo 13 de la Convención Americana (párr. 14).

Por su parte, el Consejo de Derechos Humanos de la Organización de las Naciones Unidas, en su resolución titulada *Promoción, protección y disfrute de los derechos humanos en Internet* A/HRC/20/L.13, de 29 de junio de 2012[20], determinó que:

> […] los derechos de las personas también deben estar protegidos en Internet, en particular la libertad de expresión, que es aplicable sin consideración de fronteras y por cualquier procedimiento que se elija, de conformidad con el artículo 19 de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos (pág 2).

Los relatores para la libertad de expresión de las Naciones Unidas, de la Organización para la Seguridad y Cooperación en Europa, de la Organización de los Estados Americanos y de la Comisión Africana de Derechos Humanos y de los Pueblos, en una declaración conjunta emitida en mayo de 2014 señalaron que: el "[…] rol clave [de Internet] para posibilitar la universalidad de la libertad de expresión"[21]. En la misma ocasión, los Relatores identificaron ciertos principios mínimos para asegurar la libertad de expresión en Internet, entre otros:

a) Internet es objeto de protección, en tanto sea considerado un medio que permite el ejercicio del derecho a la libertad de expresión;

b) Toda restricción a este derecho debe aplicarse con particular cautela y se debe considerar que una restricción en una jurisdicción determinada podría tener efectos en otras; y,

c) Es deber de los Estados la promoción activa de un acceso universal a Internet, con completo apego y respeto al principio de neutralidad en la red y la no discriminación.

Ya anteriormente, estos relatores habían destacado que al examinar la proporcionalidad de una restricción a la libertad de expresión en Internet se debe: "[…] ponderar el impacto que dicha restricción podría tener en la capacidad de Internet

20 A/HRC/20/L.13, de 29 de junio de 2012, disponible en: http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_20_L13.pdf.

21 Declaración Conjunta sobre universalidad y el derecho a la libertad de expresión. Firmada por Relator Especial sobre la Libertad de Opinión y Expresión de la ONU, el Representante para la Libertad de Prensa de la OSCE, la Relatora Especial sobre la Libertad de Expresión de la OEA y la Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la CADHP el 6 de mayo de 2014, literal h).

para garantizar y promover la libertad de expresión respecto de los beneficios que la restricción reportaría para la protección de otros intereses”[22].

También en 2014, un grupo de 63 organizaciones de la sociedad civil, solicitó al Consejo de Derechos Humanos de la Organización de Naciones Unidas que recuerde a los Estados su obligación de: “[…] promover y facilitar un acceso a Internet universal, equitativo, asequible y de alta calidad, basándose en los derechos humanos, el Estado de Derecho y la neutralidad en la red, incluso durante épocas de disturbios”[23]. En tal ocasión, además, se expresó la preocupación de la sociedad civil por los bloqueos de comunicaciones, la vigilancia no autorizada a los usuarios, la intercepción de las comunicaciones, entre otras, por constituir vulneraciones a la libertad de expresión.

Respecto de la posible limitación penal de la difusión de información y opiniones en Internet bajo el argumento de preservar derechos de las personas, pero con el propósito velado de impedir el debate sobre cuestiones de interés público, vale la pena recordar el estándar desarrollado por la Corte Interamericana en el caso Kimel v. Argentina[24]:

> […] el Estado no sólo debe minimizar las restricciones a la circulación de la información sino también equilibrar, en la mayor medida posible, la participación de las distintas corrientes en el debate público, impulsando el pluralismo informativo. En consecuencia, la equidad debe regir el flujo informativo.
>
> […] Respecto al grado de afectación de la libertad de expresión, la Corte considera que las consecuencias del proceso penal en sí mismo, la imposición de la sanción, la inscripción en el registro de antecedentes penales, el riesgo latente de posible pérdida de la libertad personal y el efecto estigmatizador de la condena penal […] demuestran que las responsabilidades ulteriores establecidas […] fueron graves. Incluso la multa constituye, por sí misma, una afectación grave de la libertad de expresión, dada su alta cuantía.
>
> […] En la arena del debate sobre temas de alto interés público, no sólo

---

22 Declaración Conjunta sobre Libertad de Expresión e Internet. Firmada por el Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión, la Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Relatora Especial de la Organización de Estados Americanos (OEA) para la Libertad de Expresión y la Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP) el 1 de junio de 2011, punto 1, literal b.

23 63 grupos de la sociedad civil piden que la ONU proteja la libertad de expresión en la red, disponible en: http://www.article19.org/data/files/annual_reports_and_accounts/Oral_Statement.pdf.

24 Corte IDH. Caso Kimel Vs. Argentina. Fondo, Reparaciones y Costas. Sentencia de 2 de mayo de 2008. Serie C No. 177.

> se protege la emisión de expresiones inofensivas o bien recibidas por la opinión pública, sino también la de aquellas que chocan, irritan o inquietan a los funcionarios públicos o a un sector cualquiera de la población. En una sociedad democrática, la prensa debe informar ampliamente sobre cuestiones de interés público, que afectan bienes sociales, y los funcionarios rendir cuentas de su actuación en el ejercicio de sus tareas públicas.

En el mismo sentido, el principio 5 de la Declaración de Principios sobre Libertad de Expresión de la CIDH dispone que: "[l]as restricciones en la circulación libre de ideas y opiniones, como así también la imposición arbitraria de información y la creación de obstáculos al libre flujo informativo, violan el derecho a la libertad de expresión"[25].

La misma relatoría expresó en su informe del año 2014 sobre Libertad de Expresión e Internet que "el derecho a la jurisdicción de los Estados para la persecución de delitos no debe convertirse en una medida de limitación indirecta que amedrente la libre circulación de información ante la amenaza de múltiples litigios y sanciones en diferentes jurisdicciones" (párr. 67) y que "no sería aceptable una ley que penalice, específicamente, los delitos contra el honor en línea e imponga penas más rigurosas que para los perpetrados en el mundo offline" (párr. 74).

En su Declaración Conjunta sobre Libertad de Expresión en Internet de enero del año 2012[26], las relatorías de la ONU y la OEA sobre la materia consideraron que:

> [...] los Estados deberían tener presente que si bien la libertad de expresión puede ser restringida para conseguir objetivos legítimos, como la prevención de delitos o la protección de los derechos de los demás, tales limitaciones deben ser redactadas de manera clara y precisa y afectar en el menor grado posible el derecho a la libertad de expresión. Cualquier medida que afecte las expresiones que circulan en Internet, debería concebirse con la finalidad específica de preservar la capacidad singular de este medio para promover la libertad de expresión a través del intercambio libre de información e ideas en forma instantánea y a bajo costo, sin consideración de fronteras.

Asimismo, la relatoría especial de la OEA ha cuestionado que se extienda el concepto de delitos informáticos a conductas que no comprometan directamente la infraestructura y la información almacenada o de cualquier manera administrada a través de Internet, incluyendo el uso de medios tecnológicos como instrumento para cometer un ilícito de cualquier naturaleza, pues tal inclusión pudiera implicar la criminalización del uso de Internet. En este sentido, ha expresado que debe

25 CIDH. Declaración de Principios sobre Libertad de Expresión, disponible en: http://www.oas.org/ES/CIDH/EXPRESION/showarticle.asp?artID=26&lID=2.

26 Declaración conjunta del 20 de enero de 2012, disponible en: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=888&lID=2

evitarse que conductas como la difamación o el fraude sean considerados delitos informáticos o que la sanción de estos delitos resulte agravada por el simple uso de medios tecnológicos para cometerlos[27].

A pesar de que en ciertas circunstancias pudiera resultar legítimo el uso excepcional de programas o sistemas de vigilancia de las comunicaciones para satisfacer fines como la prevención del delito, estas restricciones deben ser estrictamente proporcionadas al objetivo que persiguen y deben cumplir con las normas del derecho interno e internacional sobre libertad de expresión. Por ende, las causales para tal monitoreo siempre deberían estar taxativamente contempladas en la ley, la vigilancia debería tener una limitación temporal, ser expresamente autorizada y controlada por una autoridad judicial y, una vez concluida, toda la información obtenida que no fuera relevante para sustentar una eventual acusación, tendría que ser destruida. Estas cuestiones fueron parte de la discusión en el marco del *caso Escher e outros v. Brasil* resuelto en el año 2009[28].

En relación con lo anterior, la relatoría especial de la OEA, en su informe anual del año 2009, consideró que para la vigilancia de actividades en Internet se invocan razones de seguridad nacional y de lucha contra el delito o el crimen organizado:

> […] la ley, para limitar el ejercicio de interpretaciones discrecionales, debe especificar claramente los criterios que deben aplicarse para determinar los casos en los cuales este tipo de limitaciones resultan legítimas y ser cuidadosa en definir con exactitud dicho concepto. En particular, la Relatoría Especial ha afirmado que el concepto de seguridad nacional no puede ser interpretado de cualquier forma y debe ser definido desde una perspectiva democrática[29].

Por último, cuando se está frente a contenidos abiertamente delictivos o a discursos no protegidos por la libertad de expresión (por ejemplo la propaganda de guerra y la apología del odio que constituya incitación a la violencia), es admisible la adopción de medidas de bloqueo y filtrado de contenidos específicos. En estos casos, la medida debe someterse a un estricto juicio de proporcionalidad y estar diseñada y limitada de manera que no alcance a discursos legítimos que merecen protección. En otras palabras, las medidas de filtrado o bloqueo deben diseñarse y aplicarse de modo tal que impacten, exclusivamente, el contenido reputado ilegítimo, sin afectar otros contenidos.

---

27 CIDH. Informe sobre Libertad de Expresión e Internet, disponible en: http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_web.pdf, párrs 119 y ss.

28 CORTE IDH. *Caso Escher e outros v. Brasil.* Sentencia del 6 de Julio de 2009. Serie A No. 200, disponible en: http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf

29 CIDH, Informe anual de la Relatoría Especial para la Libertad de Expresión, año 2009, disponible en: http://www.oas.org/es/cidh/expresion/docs/informes/anuales/Informe%20Anual%202009%201%20ESP.pdf, párr. 76.

8. Corolario

Históricamente el derecho penal se ha debatido entre periodos liberales y periodos autoritarios (Zaffaroni, 2004). Al momento, vivimos una nueva era de panpenalismo y eficientismo penal en que las sociedades de nuevo consideran que la intervención policiva del Estado es la panacea que resolverá los problemas de la humanidad, ese fenómeno que Ferrajoli llama "inflación penal". Por eso mismo, debemos tener mucho cuidado con la tentación de punir los ejercicios legítimos de derechos tan elementales como la libertad de expresión. La lógica detrás de la existencia de una supercarretera de la información a la que todos podamos acceder sin restricciones, se sustenta justamente en la libertad y la igualdad. Por eso, "las características especiales que han hecho de Internet un medio privilegiado para el ejercicio cada vez más democrático, abierto, plural y expansivo de la libertad de expresión, deben ser tenidas en cuenta al momento de establecer cualquier medida que pueda impactarla" (CIDH, 2013, p. 6).

Es entonces necesario reflexionar si el recurso a la tipificación penal, frente a ciertos usos del Internet que pudieran ser legítimos y no tener el propósito de ocasionar un daño determinado, se justifica o no, en atención a los principios de *ultima ratio* y de intervención mínima del Derecho Penal. La experiencia enseña que el abuso de los instrumentos punitivos tarde o temprano se vuelve un problema mayor, sin duda es más inteligente diseñar normas jurídicas no penales para atender las necesidades de protección a ciertos intereses individuales y/o colectivos.

El alto nivel de fragmentación y polarización política de la sociedad internacional contemporánea genera serios cuestionamientos a las posibilidades reales de una cooperación eficiente en la persecución de fenómenos delictivos que más allá de ser complejos por sus tecnicismos y por el escenario virtual en el que ocurren, plantean una serie de desafíos procesales ya descritos en secciones precedentes.

El encuadramiento de algunas conductas ilícitas cometidas en o través del Internet en tipos penales tradicionales ya contemplados en la legislación penal doméstica generan un riesgo elevado de analogía in *malam partem*.

Más allá de la adopción de normativa penal sustantiva para castigar este tipo de conductas, su investigación exige una metodología particular y su sanción, en ciertos casos, un procedimiento diferenciado, de lo que en general, hasta ahora, las legislaciones locales no se han ocupado.

Por lo pronto, la respuesta penal ecuatoriana frente al aumento de los ilícitos en o a través de Internet es todavía tímida, procura emular experiencias ajenas y distantes, tiene una técnica legislativa pobre, pero finalmente, como dice la sabiduría popular, "es lo que hay". El desafío, entonces, radica en educar a los operadores de justicia y diseñar estrategias para que la interpretación y aplicación de las normas que tipifican delitos cibernéticos no resulte ni abusiva ni diminuta, ¡en eso estamos!

Bibliografía:

ALBÁN GÓMEZ, E. (2015). *Manual de Derecho Penal Ecuatoriano*. Tomo I Parte General – Código Orgánico Integral Penal. Quito. Primera Edición. Ediciones Legales.

BENÍTEZ ORTÚZAR, I. (2008). *Informática y delito. Aspectos penales relacionados con las nuevas tecnologías*, en *Reforma del Código Penal. Respuestas para una sociedad del siglo XXI*. Madrid. Dykinson.

BUSTOS, J y HORMAZABAL, H. (1997). *Lecciones de derecho penal*. Segunda Edición. Madrid. Editorial Trotta.

CIDH. (2013). *Libertad de expresión e Internet*. OEA/Ser.L/V/II. CIDH/RELE/INF. 11/13. Washington DC.

CORTÉS CASTILLO, C. (2014). *Internet y derechos humanos: aportes para la discusión en América Latina / Carlos Cortés Castillo y Eduardo Andrés Bertoni; compilado por Eduardo Andrés Bertoni*. Primera Edición. Buenos Aires. Del Puerto.

CRUZ DE PABLO, J. (2006). *Derecho penal y nuevas tecnologías. Aspectos sustantivos*. Madrid. Grupo Difusión.

LÓPEZ ZAMORA, P. (2006). *El Ciberespacio y su ordenación*. Primera Edición. Madrid. Lex Nova.

MIRÓ LLINARES, F. (2011). *La oportunidad criminal en el Ciberespacio*. Revista Electrónica de Ciencia Penal y Criminología, Número 13.

MIRÓ LLINARES, F. (2013). *La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el Ciberespacio*, Revista Española de Investigación Criminológica, (11), pp. 5 ss.

MOLES PLAZA, R. (2004). *Derecho y control en Internet. La regulabilidad en Internet.* Barcelona. Ariel Derecho.

PIÑAR MAÑAS, J. (2011). *El derecho fundamental a la protección de datos y la privacidad de los menores en las redes sociales*, en PIÑAR MAÑAS, J. (dir.), Redes sociales y privacidad del menor. Madrid. Editorial Reus.

RODRÍGUEZ-MAGARIÑOS, F. (2008). *Nuevos delitos informáticos: phising, pharming, hacking y cracking*. SP/DOCT/3705. Madrid. Ilustre Colegio de Abogados de Madrid.

VELASCO NÚÑEZ, E. (2010). *Delitos cometidos a través de Internet. Cuestiones procesales*. Madrid. Editorial La Ley.

ZAFFARONI, E. (2004). *El derecho penal liberal y sus enemigos*, manuscrito de su intervención con motivo de recibir el título de Doctor *honoris causae* de la Universidad de Castilla La Mancha, Toledo.

Las telecomunicaciones en desastres: el deber de facilitar y proteger el uso del internet

Hugo Cahueñas Muñoz
Universidad San Francisco de Quito

RESUMEN: Este artículo analiza el uso de las telecomunicaciones en situaciones de desastre. El documento detalla algunos instrumentos internacionales y describe ciertos elementos destacables de derecho comparado. Posteriormente, se identifican las normas ecuatorianas en el sector de las telecomunicaciones. Finalmente, se describe la respuesta de este sector luego del terremoto ocurrido el 16 de abril en Ecuador. La investigación propone el uso a cero costo de servicios y aplicaciones que puedan contribuir en las tareas de respuesta durante un desastre.

PALABRAS CLAVE: Desastres, telecomunicaciones, asistencia humanitaria, internet, emergencias, cero costo.

ABSTRACT: This paper analyzes the use of telecommunications in disaster situations. The document details some international and comparative law instruments. Later, the Ecuadorian standards in the telecommunications sector will be identified. Finally, the paper will describe the response of this sector after the ear-

thquake in Ecuador on April 16. The research proposes the zero rating use of services and applications that can contribute to response efforts during a disaster

KEYWORDS: Disasters, telecommunications, humanitarian assistance, internet, emergencies, zero rating.

1. Introducción

El 16 de abril de 2016, un terremoto de 7.8 grados se registró en la costa de Ecuador. Muchas personas se enteraron del sismo por medio de las redes sociales, durante varias horas, este fue su único medio de comunicación con sus familiares y amigos que fueron víctimas de este desastre natural. Ciertas redes sociales pusieron a disposición sus servicios de comunicaciones para situaciones de emergencias. Por ejemplo Facebook y Google, inmediatamente, activaron sus sistemas de búsqueda de personas.[1] Sin embargo, en las redes sociales se vivió el tercer desastre[2]: al no contar con medios de comunicación específicos se generó mucha desinformación y no se aprovecharon todas las herramientas que brinda la tecnología. Las telecomunicaciones son decisivas en todas las etapas de la gestión de un desastre. Inclusive, antes de que ocurra un desastre, las telecomunicaciones pueden transmitir información sobre la inminencia de un peligro, con el fin de que se tomen todas las precauciones necesarias para mitigar sus consecuencias (Ministerio de Comunicaciones, 2008, p. 6). Cuando se produce el desastre, las telecomunicaciones pueden contribuir para coordinar las operaciones de respuesta y recuperación efectuadas por las entidades nacionales y la comunidad internacional. (Ministerio de Comunicaciones, 2008, p. 6). Es decir, las telecomunicaciones juegan un rol importante en el ciclo de la gestión de riesgo de desastres: preparación, respuesta y recuperación.

El presente artículo se centra en la fase de respuesta del desastre, en la que, los organismos de socorro deben saber el número de heridos o fallecidos, cuántas personas necesitan asistencia médica o deben ser transportadas a centros médicos, en dónde existen personas sepultadas por estructuras colapsadas y dónde se necesi-

---

1 Facebook habilitó una versión de la verificación de seguridad que permitió a las personas residentes en la zona del desastre compartir los mensajes de indicando que están bien. El buscador de personas de Google ayudó a las personas a reconectarse con amigos y seres queridos en las consecuencias de los desastres naturales y humanitarios. (Por ejemplo, ver: Google, "Google person finder" Http://google.org/personfinder/global/home.html, >, [22/06/2016])

2 Se denomina como primer desastre al evento adverso en sí, en el presente caso es el terremoto. El segundo desastre es la asistencia humanitaria carente de organización. La llegada de personas y bienes genera un caos en la zona del desastre. Por ejemplo, quienes asisten se convierten en víctimas por la falta de preparación y organización. (Ver: Islam, M. Et. al, "Who Is Responsible for the "Second Disaster"?", Stanford Social Innovation Review <http://ssir.org/articles/entry/who_is_responsible_for_the_second_disaster>, [07/07/2016].).

.

tan, con más urgencia, equipos de búsqueda y socorro. Esta información debe ser compartida con todas las autoridades gubernamentales y los organismos humanitarios que participan en la respuesta (Delgado, s/d, p.3).

En primer lugar, se detallará los instrumentos internacionales y regionales relacionados con las telecomunicaciones en la respuesta a desastres. Luego, a manera de ejemplo, se describen los elementos destacables de derecho comparado, tomando como muestra países en los que se han registrado terremotos en los últimos años, así como un ejemplo de un país vecino. Posteriormente, se identifican las normas ecuatorianas en el sector de las telecomunicaciones; y, finalmente, se describirá la respuesta de este sector, luego del terremoto ocurrido el 16 de abril en Ecuador. A manera de cierre, se presentan algunas recomendaciones.

2. Telecomunicaciones y desastres en el derecho internacional y regional

Las telecomunicaciones juegan un papel muy importante en el monitoreo de amenazas naturales, en el envío de alertas tempranas y en la coordinación de las operaciones de respuesta ante desastres naturales (ITU, 2013, p.13). La relación entre telecomunicaciones y emergencias ha sido reconocida por el derecho internacional desde el siglo XIX. Así, en 1865, el tratado internacional que creó la Unión Telegráfica Internacional establecía que una emergencia puede justificar la interrupción de una transmisión (Fisher, 2007a, p. 43). Este rol pasivo de las telecomunicaciones ante las emergencias y desastres trasciende a un rol activo en la respuesta a emergencias. En 1998, específicamente, se adoptó el más importante instrumento internacional relativo a las operaciones internacionales de asistencia humanitaria y telecomunicaciones: el Convenio de Tampere que trata sobre el suministro de las telecomunicaciones para la mitigación de catástrofes y las operaciones de socorro (Convenio de Tampere). Este convenio señala que los Estados Partes tienen la obligación de reducir las barreras regulatorias al uso de las telecomunicaciones para la mitigación y asistencia ante desastres, además, se incluyen las restricciones a la importación y exportación de los equipos (Fisher, 2007a, p. 43-44).

Cabe señalar que el Convenio de Tampere se aplica a Estados y a otras entidades que proveen socorro, se incluyen también las organizaciones humanitarias, quienes se deberían beneficiar de los privilegios y facilidades en materia de telecomunicaciones en el escenario de un desastre. A nivel internacional, Ecuador es miembro de la Unión Internacional de Telecomunicaciones (UIT) y también de la Comisión Interamericana de Telecomunicaciones (CITEL); sin embargo, Ecuador no ha firmado el Convenio de Tampere.

En el seno de la UIT se destacan varias resoluciones y recomendaciones relevantes para la respuesta a desastres naturales (Fisher, 2007b, p. 9). En 2006, la re-

solución 36, "Las Telecomunicaciones/[Tecnologías de la Información y las Comunicaciones]TIC al servicio de la asistencia humanitaria", invitó a los Estados miembros a adherirse al Convenio de Tampere, como cuestión de prioridad, y también a tomar todas las medidas prácticas para la aplicación de referido Convenio (UIT, 2006a). En el mismo año, se adoptó la resolución denominada "El uso de las TIC para el seguimiento y la gestión en situaciones de emergencia y de desastre para la alerta temprana, prevención, mitigación y recuperación" (UIT, 2006b). Entre otros aspectos, esta resolución alienta a los Estados miembros a:

> [Q]ue faciliten la utilización por organizaciones de emergencia, de tecnologías y soluciones existentes y nuevas (por satélite y terrenales), en la medida de lo posible, con el fin de satisfacer los requisitos de interfuncionamiento y alcanzar los objetivos de protección pública y operaciones de socorro (UIT, 2006b).

En 2010, la UIT adoptó la resolución 34 llamada: "El papel de las telecomunicaciones/TIC en la alerta temprana, mitigación de desastres y ayuda humanitaria". En esta resolución se solicitó a la oficina de Desarrollo de las Telecomunicaciones de la UIT "apoyar a las administraciones en su labor hacia la aplicación del Convenio de Tampere"; además, la UIT debe "reforzar el vínculo entre el desarrollo de las telecomunicaciones y los desastres" (UIT, 2010, p.84).

A nivel interamericano, cabe destacar que, de conformidad con el artículo 53 de la Carta de la Organización de los Estados Americanos (OEA), la Asamblea General estableció la CITEL (OEA, 1993). Por un lado, el Comité Directivo Permanente de la CITEL (COM/CITEL) ha insistido a sus Estados miembros en la necesidad de firmar, ratificar y aplicar el Convenio de Tampere (COM/CITEL, 1999; COM/CITEL, 2003). Por otro lado, la CITEL tiene como función "[a]poyar la preparación para desastres y servir como medio para que los Estados Miembros canalicen sus necesidades de telecomunicaciones en relación con alerta temprana, mitigación y recuperación de desastres naturales" (CITEL, 2014, p. 3). Además, en 2015, la Secretaría Ejecutiva de la CITEL planteó una alianza regional por la seguridad y emergencia con las TIC, en las que se propone la disponibilidad de espectro de las redes de banda ancha para desastres, seguridad y emergencias (COM/CITEL, 2015, p.2).

Dentro de la OEA, el Comité Consultivo Permanente III: Radiocomunicaciones de la CITEL (CCP.III) recomendó:

> 1. Que cada uno de los países debe desarrollar un plan nacional consolidado de preparación para identificar recursos capaces de proveer comunicación de emergencia, bosquejar los pasos necesarios para mitigar el daño a esos recursos, establecer medios para proveer servicios temporales y realizar provisiones para recuperarse del desastre.
>
> [...] 3. Que las redes de comunicaciones para desastres se prueben regularmente a nivel nacional y regional bajo condiciones de emergencia simu-

> ladas, incluyendo enlaces de conexión entre los centros de huracán y los centros regionales de emergencia […] (CCP.III, 1996, p.20)

Se agrega a estos antecedentes que, en 2007, la Conferencia Internacional de la Cruz Roja, integrada también por los Estados partes de los Convenios de Ginebra[3], adoptó de manera unánime las "Directrices para la facilitación y reglamentación nacionales de socorro en casos de desastre y asistencia para la recuperación inicial" (Directrices IDRL por sus siglas en ingles).[4] En relación con las telecomunicaciones, las Directrices IDRL señalan que

> […] los Estados afectados deberían […] conceder (o cuando corresponda alentar a otros actores nacionales a conceder) a los Estados que prestan asistencia y a las organizaciones humanitarias […] un acceso prioritario al ancho de banda, las frecuencias y el uso de satélites para las telecomunicaciones y la transmisión de datos relacionados con las operaciones de socorro en casos de desastre (Directrices IDRL, 18.2).

Adicionalmente, la importancia de la tecnología en la gestión de riesgo de desastres ha sido reconocida en recientes instrumentos internacionales. En primer lugar, el Marco de Sendai para la Reducción del Riesgo de Desastres (2015-2030) señala la importancia de

> […] reforzar la utilización de los medios de comunicación, incluidas las redes sociales, los medios tradicionales, los macrodatos y las redes de telefonía móvil, en apoyo de las medidas nacionales para una comunicación efectiva de los riesgos de desastres, como corresponda y de conformidad con la legislación nacional[…] (Asamblea General de Naciones Unidas, 2015a, Anexo II, 25. C).

En segundo lugar, la Agenda 2030 para el Desarrollo Sostenible incluye el objetivo "[c]onstruir infraestructuras resilientes, promover la industrialización inclusiva y sostenible y fomentar la innovación" (Asamblea General de Naciones Unidas, 2015b, Objetivo 9), para lo cual es necesario "aumentar de forma significativa el acceso a la tecnología de la información y las comunicaciones y esforzarse por facilitar el acceso universal y asequible a Internet en los países menos adelantados a más tardar en 2020 (9.c). Esto podría interpretarse también como la necesidad de construir infraestructura resiliente para las telecomunicaciones (ITU, 2013, p.15) y, en particular, para el servicio de internet.

3. Derecho comparado

Si se toma en cuenta el derecho comparado, es necesario destacar la normativa

3 Incluida la República del Ecuador.

4 La Asamblea General de la Organización de las Naciones Unidas adoptó tres resoluciones (Res. 63/139, 63/141 y 63/137) en las que se alienta a los Estados a hacer uso de las Directrices IDRL.

de Japón y Chile, por ser los países sísmicamente más activos del mundo y que han vivido, en años recientes, terremotos de similar magnitud y consecuencias al ocurrido en Ecuador. Además, Colombia se destaca por ser un país vecino que cuenta con un plan de contingencia para el sector de telecomunicaciones que brinda luces para el análisis del sector ecuatoriano.

En Japón, la legislación sobre telecomunicaciones establece que las compañías de telecomunicaciones deben dar prioridad a las comunicaciones cuyo contenido ayude a la prevención o alivio de calamidades (Ley de Comercio de Telecomunicaciones de Japón, art. 8). Adicionalmente, la ley que regula la gestión de riesgos de desastres señala que el alcalde de una ciudad tiene la obligación de informar la alerta de un desastre a todas las personas residentes dentro de su jurisdicción (Ley de Contramedidas a Desastres de Japón, art. 56). Estas comunicaciones tendrán prioridad frente a las otras comunicaciones de carácter comercial y pueden solicitar la emisión de mensajes mediante instalaciones de comunicaciones eléctricas o instalaciones de radio (Ley de Contramedidas a Desastres de Japón, art. 57). En la actualidad, como parte del sistema de alerta temprana se envían mensajes o correos a los celulares, lo cual no genera un costo por el mensaje o por el servicio (Fukahori, 2012, p.24).

Luego del terremoto de 2011, en la evaluación de las telecomunicaciones, este país asiático estableció como prioridad que, en tiempo de desastres, se flexibilice la reconfiguración de los recursos del proceso de comunicación, para así, maximizar los posibles recursos que pueden dirigirse a los servicios de comunicación durante el desastre, es decir, priorizar las comunicaciones de voz y correo, y limitar la comunicación de medios interactivos como música, video y archivos (Fukahori, 2012, p. 46).

Chile, al igual que Ecuador, es un país andino ubicado en el cinturón del fuego del Pacífico. Su ley de telecomunicaciones ha establecido disposiciones específicas con relación a los desastres naturales. Respecto a los costos de transmisión de mensajes en situación de desastre la ley señala que:

> Los concesionarios, permisionarios o licenciatarios de telecomunicaciones deberán transmitir sin costo, en la medida que sus sistemas técnicos así lo permitan y en que no se afecte la calidad de servicio [...] los mensajes de alerta que les encomienden el o los órganos a los que la ley otorgue esta facultad. Lo anterior con el fin de permitir el ejercicio de las funciones gubernamentales de coordinación, prevención y solución de los efectos que puedan producirse en situaciones de emergencia [...] (art. 7º bis.)

Como parte de la preparación ante desastres, la Subsecretaría de Telecomunicaciones debe desarrollar un "plan de resguardo de la infraestructura crítica de telecomunicaciones del país, con el objeto de asegurar la continuidad de las comunicaciones en situaciones de emergencia:[...]" (art. 39. A). El plan de contingencia

incluye la obligación de identificar las estructuras críticas (art. 39. A. b) y establecer medidas de resguardo para esta estructura (art. 39.A. c). Es decir, la infraestructura del sector de telecomunicaciones debe ser resiliente frente a los desastres naturales o emergencias.

El reglamento de la ley de telecomunicaciones de Chile menciona nuevamente la exención de un "pago para las comunicaciones efectuadas por el usuario de servicios públicos de voz, destinados a los niveles especiales de servicios de emergencia y otros definidos por la normativa" (art. 21); sin embargo, no se contempla una exención similar para el internet o datos en la telefonía móvil.

En Colombia, para los casos de atención de emergencias o desastres, la Ley 1341, por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las TIC, dicta que:

> Los proveedores de redes y servicios de telecomunicaciones deberán poner a disposición de las autoridades de manera gratuita y oportuna, las redes y servicios y darán prelación a dichas autoridades en la transmisión de las comunicaciones que aquellas requieran. En cualquier caso se dará prelación absoluta a las transmisiones relacionadas con la protección de la vida humana. Igualmente darán prelación a las autoridades en la transmisión de comunicaciones gratuitas y oportunas para efectos de prevención de desastres, cuando aquellas se consideren indispensables (art.8).

El mismo artículo señala que los proveedores de redes y servicios de telecomunicaciones tienen la obligación de "suministrar a las autoridades competentes, sin costo alguno, la información disponible de identificación y de localización del usuario que la entidad solicitante considere útil y relevante para garantizar la atención eficiente en los [desastres o emergencias]" (art.8).

Se observa que en la legislación colombiana, el enfoque de la gratuidad es para las instituciones estatales, no para los usuarios. Cabe destacar que los proveedores deben suministrar información disponible de identificación y localización de usuarios, lo cual puede ser muy útil en las tareas de búsqueda de los equipos de rescate.

Adicionalmente, Colombia cuenta con un plan de contingencia para el sector de telecomunicaciones. Dentro de las acciones de este plan se contempla la siguiente:

> Fortalecer la infraestructura y la operación de las redes públicas y fomentar la adecuada, oportuna y eficiente prestación de los Servicios de Valor Agregado, como el Internet y los sistemas de banda ancha, con el fin de soportar debidamente las telecomunicaciones en casos de emergencias y desastres (Ministerio de Comunicaciones, 2008, p.64).

Este plan reconoce que "es incuestionable la posibilidad de empleo y aplicación de Internet en las telecomunicaciones de emergencia" (2008, p. 82) y se identifican

algunas formas en las que el Internet puede servir de apoyo a las operaciones de socorro en situaciones de desastre, por ejemplo:

i. Enviar y recibir correos electrónicos y utilizar directorios de la Web para localizar a colegas, proveedores y organizaciones gubernamentales y no gubernamentales que pueden prestar asistencia.

ii. Seguir de cerca las noticias y la información meteorológica procedentes de una serie de entidades gubernamentales, académicas y comerciales.

iii. Obtener información geopolítica actualizada, mapas geográficos, avisos de viaje, boletines e informes sobre la situación relativa a sectores de interés.

iv. Consultar bases de datos médicos para reunir información completa sobre casos que van desde las infecciones parasitarias hasta las heridas graves.

v. Participar en listas de discusión mundiales para intercambiar la experiencia adquirida y coordinar las actividades.

vi. Leer y hacer comentarios sobre el contenido de varios sitios Web, gubernamentales y no gubernamentales, para tener conocimiento de la situación general y del modo en que otros están describiendo la catástrofe.

vii. Registrar a los refugiados y desplazados para facilitar su reunión con familiares y amigos. (2008, p. 82-83).

Respecto a los sistemas de banda ancha inalámbrica, el plan de contingencia manifiesta que estos sistemas constituyen una alternativa válida para cubrir zonas remotas donde no existen centros de comunicación y de conectividad. Los sistemas de banda ancha inalámbrica pueden utilizarse para todo tipo de comunicaciones, incluidas voz, datos, imágenes y video (2008, p. 83). Además, estas redes admiten y soportan aplicaciones y servicios de telecomunicaciones en convergencia como: internet, radio y videoconferencia (2008, p. 83). Específicamente, se destaca que las TIC, basadas en la banda ancha inalámbrica e internet, permiten la implantación y el desarrollo del "Sistema Integrado de Información", el cual tiene como objeto:

> Sistematizar el inventario y la información existente sobre amenazas y riesgos para la planificación y de la información histórica de desastres y pérdidas en el territorio nacional, sistematizar la información relativa a sistemas de vigilancia, alerta, diagnóstico temprano e inventario de recursos para la reacción institucional efectiva y sistematizar la información sobre manejo y transporte de sustancias peligrosas. (Decreto 93 de Colombia, art. 7.3.7).

Estas buenas prácticas en derecho comparado de países con amplia experiencia en la respuesta a desastres naturales brindan elementos para el análisis de la legislación ecuatoriana. Además, se podrían iniciar procesos de cooperación en materia de telecomunicaciones y gestión de riesgo de desastres. Se destaca que

Ecuador mantiene acuerdos bilaterales en materia de gestión de riesgo con Chile y Colombia. Con Chile existe un acuerdo marco de cooperación interinstitucional entre el Ministerio de Coordinación de Seguridad, el Ministerio del Interior y la Secretaría Nacional de Gestión de Riesgos de Ecuador, y el Ministerio del Interior y Seguridad Pública de Chile, mediante este acuerdo se estableció un régimen de cooperación técnica para la transferencia de experiencias y buenas prácticas en la prevención y enfrentamiento de desastres naturales (Cahueñas-Muñoz, 2013, p. 16). Con Colombia se destacan dos instrumentos internacionales: en 1990, se suscribió un acuerdo sobre desastres naturales, en el cual ambos países se comprometían a desarrollar acciones de cooperación entre los sistemas nacionales de gestión de riesgo de desastres; además, en caso de catástrofe real o inminente, el otro país pondría a disposición sus sistemas de monitoreo, comunicación y alerta (Cahueñas-Muñoz, 2013, p. 15).

4. Telecomunicaciones y desastres en el derecho ecuatoriano

En el sistema jurídico ecuatoriano, el acceso universal a las TIC es un derecho fundamental reconocido por la Constitución (art.16.2). Complementariamente, se establece que en el campo de las telecomunicaciones el Estado central tiene competencia exclusiva (art. 261). Además, en relación a la gestión de riesgo, el Estado tiene el deber de proteger

> a las personas, las colectividades y la naturaleza frente a los efectos negativos de los desastres de origen natural o antrópico mediante la prevención ante el riesgo, la mitigación de desastres, la recuperación y mejoramiento de las condiciones sociales, económicas y ambientales, con el objetivo de minimizar la condición de vulnerabilidad (Constitución de la República del Ecuador, art.389).

Para el cumplimiento de esta obligación, la rectoría de la gestión de riesgos la ejerce el Estado, a través de un organismo técnico establecido por Ley (Constitución de la República del Ecuador, art. 389); sin embargo, los riesgos se gestionan por el principio de descentralización subsidiaria, mediante el cual, las instituciones son responsables dentro de su ámbito geográfico; mas, cuando sus capacidades son superadas, son las instancias de mayor ámbito territorial y mayor capacidad técnico-financiera las que brindarán el apoyo necesario (art. 390). La Ley de Seguridad Pública y del Estado, en el artículo 11.d, señala que la rectoría de la gestión de riesgos la ejercerá la Secretaría de Gestión de Riesgos (SGR). Esta Secretaría, con el objetivo de establecer las acciones que deben ejecutar las instituciones que participan en los Comités de Gestión de Riesgos/Comités de Operaciones de Emergencia (CGR/COE), emitió el Manual del Comité de Gestión de Riesgos (SGR, 2014, p.1). En referido manual se señala que el sector de telecomunicaciones es responsabilidad del Ministerio de Telecomunicaciones, el cual debe:

1. Elaborar y actualizar una base de datos sobre la infraestructura estratégica de telecomunicaciones del país.

2. Gestionar planes de reducción de riesgos para proteger la infraestructura de telecomunicaciones estratégicas del país.

3. Generar políticas, normas y estándares para asegurar la implementación de la gestión de riesgos en la planificación, ejecución, mantenimiento y evaluación de la infraestructura de telecomunicaciones estratégicas del país.

4. Fortalecimiento de capacidades en GR en las comunidades cercanas y usuarios de los servicios afines a la infraestructura de telecomunicaciones estratégicas del país. (SGR, 2014, p.86)

Cabe destacar que en la legislación secundaria ecuatoriana la Ley Orgánica de Telecomunicaciones (*en adelante* LOT) contempla dos elementos de relacionamiento entre los desastres y las telecomunicaciones. Por un lado, la ley tiene entre sus objetivos establecer los mecanismos de coordinación para atender temas relacionados con el ámbito de las telecomunicaciones en situaciones de emergencias (art. 3.17). Por otro lado, la normativa secundaria en telecomunicaciones busca "[g]arantizar que los derechos de las personas, especialmente de aquellas que constituyen grupos de atención prioritaria, sean respetados y satisfechos […]" (art. 3.14). Cabe recordar que la Constitución reconoce dentro de los grupos de atención prioritaria a las personas víctimas de desastres naturales (art. 35).

Respecto a los mecanismos de coordinación, en caso de que el decreto de estado de excepción[5] implique la necesidad de utilizar los servicios de telecomunicaciones, "los prestadores que operen redes públicas de telecomunicaciones tienen la obligación de permitir el control directo e inmediato por parte del ente rector de la defensa nacional, de los servicios de telecomunicaciones en el área afectada" (LOT, art. 8). Se observa que esta disposición mantiene un enfoque de defensa nacional, mas no de gestión de riesgo de desastres, en la que los actores y las acciones son diferentes. Sin embargo, la ley también señala que la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) regulará el alcance, los derechos, las obligaciones y el pago del valor justo del servicio utilizado por motivo de la declaración de estado de excepción (art. 8). Estas disposiciones podrían generar una contradicción si se toma en cuenta lo establecido en el Manual de Comités de Gestión de Riesgos. Evidentemente, por jerarquía normativa (Constitución del Ecuador, art. 425), deberán prevalecer las normas establecidas en la LOT sobre las mencionadas en el Manual adoptado por resolución de la SGR.

5 Se "podrá decretar el estado de excepción en todo el territorio nacional o en parte de él en caso de agresión, conflicto armado internacional o interno, grave conmoción interna, calamidad pública o desastre natural" (Constitución de la República del Ecuador, art. 164). Es oportuno decir que durante el Estado de Excepción el Presidente puede suspender o limitar el derecho a la libertad de información (Constitución de la República del Ecuador, art. 165).

Se suma a ese confuso escenario el "Reglamento para la Prestación de Servicios de Telecomunicaciones y Servicios de Radiodifusión por Suscripción" dictado por el Directorio de la ARCOTEL. En este reglamento se busca subsanar el enfoque a la defensa que se establece en la ley, separando el uso del servicio de telecomunicaciones en casos de desastre natural de las otras causales de estado de excepción. Cuando exista un desastre natural, la ARCOTEL coordinará con la autoridad competente y los prestadores de servicio (art. 32). Además, cuando el estado de excepción contemple la necesidad de utilizar los servicios de telecomunicaciones, en caso de conflicto armado o conmoción interna, así como de emergencia a nivel nacional, regional o local, "los prestadores que operen redes públicas de telecomunicaciones tienen la obligación de permitir el control directo e inmediato por parte del ente rector de la defensa nacional, de los servicios de telecomunicaciones en el área afectada [...]" (art. 33). Esta división es poco clara, porque los desastres naturales podrían incluirse dentro de las emergencias a nivel nacional, regional o local. Sin embargo, de la lectura de estos artículos se entendería que el primero se aplica en caso de desastre natural, independientemente de la declaratoria de estado de excepción. También cabe preguntarse si la "autoridad competente" para los escenarios de desastre natural es la Secretaría de Gestión de Riesgos o, si por el principio de descentralización subsidiaria, las autoridades podrían ser los Gobiernos Autónomos Descentralizados.

Concomitantemente, la ley del sector telecomunicaciones[6] establece obligaciones a los prestadores de servicios, quienes deben difundir las "alertas dispuestas por la autoridad competente [...] para casos de seguridad nacional o desastres naturales [...]" (art. 8). Específicamente, los prestadores de servicios de telecomunicaciones tienen el deber de: a) "[i]mplementar el acceso, en forma gratuita, a los servicios de emergencia, determinados por la [ARCOTEL]" (LOT**,** art. 24.11) y b) cumplir con los servicios requeridos en casos de emergencia que determine la autoridad competente; por ejemplo, llamadas gratuitas y provisión de servicios auxiliares para Seguridad pública y del Estado (LOT, art. 24.24)[7].

Complementariamente, el Reglamento del sector telecomunicaciones considera que el acceso gratuito a servicios de emergencia y la ubicación de llamadas de emergencia serán ejecutados por los prestadores del servicio de telefonía fija y servicio móvil avanzado, de conformidad con la LOT y las regulaciones de la ARCOTEL (Reglamento a la LOT, art. 59.10).

---

6 "Se entiende por telecomunicaciones toda transmisión, emisión o recepción de signos, señales, textos, vídeos, imágenes, sonidos o informaciones de cualquier naturaleza, por sistemas alámbricos, ópticos o inalámbricos, inventados o por inventarse. La presente definición no tiene carácter taxativo, en consecuencia, quedarán incluidos en la misma, cualquier medio, modalidad o tipo de transmisión derivada de la innovación tecnológica". (Ley Orgánica de Telecomunicaciones, art. 5).

7 A nivel reglamentario se establece un procedimiento para la determinación del pago por los servicios que hayan sido utilizados durante el Estado de Excepción, para lo cual se conforma una comisión técnica integrada por ARCOTEL, el Ministerio de Defensa y los prestadores de servicios (Reglamento a la Ley Orgánica de Telecomunicaciones, art. 115).

También, cabe destacar que los prestadores de servicios tienen la obligación de formular planes de contingencia para casos de desastres naturales con el objetivo de garantizar la continuidad del servicio. (LOT, art. 24.24) De hecho, no contar con un plan de contingencia constituye una infracción (LOT, art.118.7). También constituye una infracción: "no cumplir con los servicios requeridos en casos de emergencia, tales como llamadas de emergencia gratuitas, provisión de servicios auxiliares para seguridad ciudadana y cualquier otro servicio definido como servicio social o de emergencia por la [ARCOTEL]" (LOT, art.118.7)y "[n]o prestar acceso gratuito a los servicios públicos de emergencia" (LOT, art.118.20). Sin embargo, más allá de los planes de contingencia de los prestadores de servicios, se requiere un plan de contingencia de todo el sector de telecomunicaciones. Así lo identificó la SGR, que señaló que es necesario "[a]rticular los planes de contingencia para sectores estratégicos (telecomunicaciones, recursos naturales no renovables, transporte) los cuales pueden tener alta vulnerabilidad si son afectados por eventos adversos" (SGR, 2014, p. 44).

En términos de derechos, los abonados, clientes y usuarios pueden disponer gratuitamente de servicios de llamadas de emergencia (LOT, art. 22.6). Sin embargo, de la lectura de la LOT se destaca que la obligación de los presentadores del servicio de telecomunicaciones de cumplir con los servicios requeridos por ARCOTEL no es taxativa a las llamadas de emergencia. En consecuencia, podrían solicitarse otros servicios como el acceso a ciertas aplicaciones o el uso de datos. Es más, cuando la ley se refiere a las obligaciones de los abonados, clientes y usuarios lo hace en términos generales porque se refiere a los servicios de emergencia (art. 23.7).

El reglamento a la ley de telecomunicaciones y aquellos dictados por la ARCOTEL también contemplan la posibilidad de usar otros servicios de emergencia y no solo las llamadas telefónicas. Si bien, en relación con los derechos de los usuarios, el reglamento general de la LOT se refiere únicamente al derecho de acceso gratuito a servicios de llamadas de emergencia (art. 56.4) y no menciona los otros servicios que puedan ser establecidos por ARCOTEL, existe una referencia amplia cuando el reglamento habla sobre las obligaciones de los prestadores de servicios de telecomunicaciones en casos de emergencia. Específicamente, los prestadores del servicio de telecomunicaciones deben proporcionar de forma gratuita:

> i) Acceso a llamadas de emergencia por parte del abonado, cliente y usuario, independientemente de la disponibilidad de saldo; ii) <u>Difusión por cualquier medio, plataforma o tecnología, de información de alertas de emergencia a la población, conforme la regulación que emita para el efecto la ARCOTEL.</u> Dichos servicios se prestarán gratuitamente, sin perjuicio de la declaratoria de Estado de Excepción establecida en el artículo 8 de la LOT. También deberán prestar de manera obligatoria, con el pago del valor justo, lo siguiente: i) <u>Integración de sus redes a cualquier plataforma</u>

o tecnología, para la atención de servicios de emergencias, conforme a la normativa que emita la ARCOTEL; ii) Servicios auxiliares para la seguridad pública y del Estado; iii) Cualquier otro servicio que determine la ARCOTEL (art. 56.12, el subrayado me corresponde).

Cabe mencionar que la LOT busca fomentar la neutralidad de la red, lo cual protege el derecho al acceso a la información y el derecho a la no discriminación.[8] Sin embargo, esta neutralidad no se vería menoscabada porque la situación de emergencia o desastre constituye una justificación válida para permitir servicios de cero costo de ciertas aplicaciones o servicios de redes sociales. Análogamente, es importante recordar que el Ex-Consejo Nacional de Telecomunicaciones, en 2011, dictó el Reglamento para llamadas a Servicios de Emergencias, en el cual se establece que los prestadores de servicios finales de telecomunicaciones deben "[a]plicar un cargo de interconexión igual a cero (0) para llamadas de emergencia" (Art. 8.j). Un ejercicio similar se podría realizar para acceder a ciertas aplicaciones o redes sociales en situaciones de emergencia o desastre.

5. Las telecomunicaciones ante el terremoto del 16A

En respuesta al terremoto ocurrido el 16 de abril en la costa de Ecuador, el sector de las telecomunicaciones implementó varias acciones en el momento del evento y con posterioridad al mismo. En el informe de situación No. 6, de fecha 17 de abril, publicado por la SGR, se señala lo siguiente: "ARCOTEL ha dispuesto el envío de mensajes de alerta a la sociedad: Mensaje 1: Mantener la calma. Mensaje 2: Informarse a través de canales oficiales. Mensaje 3: Evacuación preventiva en zonas costeras de Esmeraldas, Manabí y Santa Elena" (SGR, 2016, p.3).

Adicionalmente, las operadoras celulares, de manera unilateral, es decir, sin el requerimiento de ARCOTEL, facilitaron el servicio de SMS gratis.[9] Esto puede ser muy positivo en la emergencia para comunicarse con sus familiares; sin embargo, la infraestructura registraba graves daños; por ejemplo, la operadora Movistar registraba una afectación en el 80% de las líneas del sector de impacto del terremoto (El Universo, 2016). Además, desde el sector público no se identificaron otros medios para comunicarse con los servicios de atención en emergencia, más allá de las llamadas telefónicas. Por ejemplo, el servicio ECU911 cuenta con una aplicación móvil por medio de la cual se pueden reportar emergencias.

Cabe mencionar que en el decreto de estado de excepción no hay una mención

8 En esta publicación, el artículo escrito por el Profesor Arturo Carrillo analiza la neutralidad de la red en términos de derechos humanos.

9 Movistar Ecuador habilitó el servicio de SMS gratis a todas las operadoras; Claro puso a disposición 1000 SMS sin costo a sus usuarios en Esmeraldas y Manabí; CNT dejó abierto el servicio de SMS gratuito para estas provincias. (El Universo, 2016)

específica para el sector telecomunicaciones.[10] En términos generales, se dispone la movilización nacional en las provincias afectadas por el sismo,

> de tal manera que todas las entidades de la Administración Pública Central e Institucional, en especial las Fuerzas Armadas y la Policía Nacional; y los gobiernos autónomos descentralizados de las provincias afectadas, deberán coordinar esfuerzos con el fin de ejecutar las acciones necesarias e indispensables para mitigar y prevenir los riesgos, así como enfrentar, recuperar y mejorar las condiciones adversas, que provoquen los eventos telúricos del día 16 de abril de 2016. (Decreto 1001, art. 2).

De acuerdo con el artículo citado y con el artículo 1 del Decreto Ejecutivo No. 1002, el 2 de mayo de 2016, es decir, 16 días luego de ocurrido el terremoto, la Directora Ejecutiva de la ARCOTEL dispuso que "durante la vigencia del estado de excepción, los cargos de interconexión disminuyan en un 50% de los valores que actualmente se tienen estipulados como cargo de terminación para todas las llamadas realizadas hacia el servicio móvil avanzado a nivel nacional" (ARCOTEL, 2016, art. 2). En el considerando de referida resolución se destaca lo siguiente:

> "las comunicaciones a través de los distintos medios como llamadas, SMS o redes sociales son de vital importancia en las actuales condiciones, no solo en las zonas afectadas sino en todo el país, [por lo que] es necesario que [...] se establezcan las condiciones en los servicios de telecomunicaciones que permitan que tanto las personas afectadas, como quienes se encuentran realizando labores de coordinación, auxilio, rescate y más temas relacionados con las consecuencias de este desastre, puedan acceder a estos servicios sin mayor costo y con facilidad" (ARCOTEL, 2016, considerando, el subrayado me pertenece).

Pese al reconocimiento de la importancia de las redes sociales para las tareas de auxilio y rescate, la resolución se adoptó cuando las tareas de búsqueda y rescate ya habían finalizado. Además, no se establece la gratuidad de ciertos servicios, por ejemplo, la citada aplicación ECU911, la cual permite solicitar auxilio a las autoridades.

6. Conclusiones y recomendaciones

- Si se tiene presente que Ecuador es miembro de UIT y CITEL, espacios que reiteradamente han sugerido la suscripción del Convenio de Tampere, se recomienda firmar y ratificar el Convenio de Tampere. En caso de no prosperar la suscripción del tratado, se deben analizar e incorporar en la legislación nacional las normas que establece referido Convenio. Se destaca el hecho de

10 Mediante Decreto Ejecutivo No. 1001 declaró el estado de excepción en Esmeraldas, Manabí, Santa Elena, Santo Domingo de los Tsáchilas, Los Ríos y Guayas.

que el Convenio de Tampere ha sido ratificado por Argentina, Colombia, Perú y Venezuela (Cahueñas-Muñoz, 2013, p.44).

- En Ecuador, la obligación de contar con planes de contingencia es de los prestadores de servicio. Al igual que Chile y Colombia, se debería incluir en la ley la obligación de desarrollar un plan de contingencia de todo el sector de telecomunicaciones. El plan debería identificar estructuras críticas y promover estructuras resilientes. Este documento debe incluir y proteger el acceso al internet y, específicamente, el uso de ciertas aplicaciones. Es necesario contemplar la experiencia colombiana al respecto. También se deberían tomar en cuenta las recomendaciones del Comité Consultivo Permanente III: Radiocomunicaciones de la CITEL. En la actualidad, en el Manual de Gestión de Riego, se establece la obligación del Ministerio de Telecomunicaciones de generar planes de reducción de riesgo, mas no de contingencia.

- Se deberían incluir los sistemas de banda ancha inalámbrica como alternativa en los planes de contingencia del sector telecomunicaciones, dado que los sistemas de banda ancha inalámbrica pueden utilizarse en zonas afectadas por un desastre para todo tipo de comunicaciones, incluidas la transmisión y recepción de voz, datos imágenes y video.

- La normativa que regule el uso de telecomunicaciones debería priorizar los servicios que se emplean en una situación de emergencia o desastre, flexibilizar la reconfiguración de los recursos del proceso de comunicación y maximizar los posibles recursos que puedan dirigirse a los servicios de comunicación durante las operaciones de auxilio y socorro. Se podría tomar como referencia la evolución que ha tenido Japón en ese ámbito.

- Se debe aclarar y corregir el enfoque hacia la defensa nacional en el sector de telecomunicaciones; tal y como ARCOTEL ha reconocido, se requiere un enfoque de gestión de riesgos para las situaciones de desastre, incluso cuando no exista un decreto de estado de excepción.

- Por un lado, la regulación de las telecomunicaciones en emergencias y desastres se ha centrado en el uso de la telefonía. Solo se regula el uso gratuito de llamadas a números de emergencia. Sin embargo, la ley y el reglamento se refieren, en términos generales, a las telecomunicaciones. Por otro lado, se presenta un creciente uso del internet, principalmente por parte de usuarios de internet móvil. En consecuencia, de conformidad con el artículo 24.11 de la Ley de Telecomunicaciones, ARCOTEL debería disponer que, de manera gratuita, se permita el uso de internet y ciertas aplicaciones en escenarios de desastres. Por ejemplo, aplicaciones como ECU911, servicios de las redes sociales como Facebook o Google, deberían ser gratuitos en situación de emergencia o desastre. Además, igual que en Colombia, los proveedores deberían tener la obligación de suministrar a las autoridades, sin costo alguno,

la información disponible de identificación y localización del usuario para garantizar la atención en el desastre o emergencia.

Bibliografía:

ARCOTEL (2016), *Resolución ARCOTEL-2016-0437* <http://www.arcotel.gob.ec/wp-content/uploads/downloads/2016/05/Resolucion-0437-ARCOTEL-2016.pdf> [07/06/2016].

Asamblea General de Naciones Unidas (2015a), *Resolución A/RES/69/283: Marco de Sendai para la Reducción del Riesgo de Desastres 2015-2030.* http://www.un.org/es/comun/docs/?symbol=A/RES/69/283.

Asamblea General de Naciones Unidas (2015b), *Resolución A/RES/70/1: Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible.* http://www.un.org/es/comun/docs/?symbol=A/RES/70/1.

Cahueñas-Muñoz, H. (2013). *Estudio sobre preparativos legales para la asistencia internacional en caso de desastre en Ecuador*. Quito: Cruz Roja Ecuatoriana-Federación Internacional de Sociedades de la Cruz Roja y de la Media Luna Roja.

CCP.III (1996), *Mejoras en las Comunicaciones para Desastres en las Américas: CCP.III/REC. 24 (VI-96)* <https://www.citel.oas.org/en/SiteAssets/PCCII/Final-Reports/P3-0580r1_e.pdf> [07/06/2016].

CITEL (2014), *Aprobación del Plan Estratégico de la CITEL:* 0BCITEL RES. 70 (VI-14)

COM/CITEL (2015), *Propuesta de Modernización de la CITEL:* COM/CITEL/doc. 018/15.

COM/CITEL(1999), *Resolución: RES.93 (VIII-99).*

COM/CITEL(2003), *Resolución: RES.169 (XIII-03).* <https://www.citel.oas.org/en/SiteAssets/About-Citel/Annual-Reports/InfAnu-2003-r3c1_e.pdf> [07/06/2016].

Constitución de la República del Ecuador 2008.

Convenio de Tampere sobre el suministro de telecomunicaciones para la mitigación de catástrofes y las operaciones de socorro.

Decreto 93 de 1998 por el cual se adopta el Plan Nacional para la Prevención y Atención de Desastres (Colombia).

Delgado, Maritze, (s/d). "CONVENIO DE TAMPERE Salvando vidas por medio de las Telecomunicaciones en Emergencias" https://www.itu.int/en/ITU-D/Emergency-Telecommunications/Documents/El_Salvador_2009/presentations/Presentación_El_Salvador_Tampere.pdf, [07/06/2016].

Directrices para la facilitación y reglamentación nacionales de socorro en casos de desastre y asistencia para la recuperación inicial-Directrices IDRL (2007). <http://www.ifrc.org/PageFiles/41203/1205600-IDRL%20Guidelines-SP-LR.pdf> [07/06/2016].

El Universo (2016) Operadoras celulares facilitan SMS tras terremoto en Ecuador http://www.eluniverso.com/vida-estilo/2016/04/17/nota/5530938/operadoras-celulares-facilitan-sms-tras-terremoto-ecuador. Domingo, 17 de abril, 2016.

Fisher, D. (2007a) *Law and legal issues in international disaster response: a desk study.* Geneva: International Federation of Red Cross and Red Crescent Societies.

Fisher, D. (2007b), Derecho y asuntos legales en la respuesta internacional a desastres: un estudio de gabinete – Versión resumen. Ginebra: Federación Internacional de Sociedades de la Cruz Roja y Media Luna Roja.

Fukahori M. (2012), *Disaster and ICT Systems in Japan. Diponible en:* https://www.itu.int/en/ITU-T/Workshops-and.../kns01-p02.ppt.

Islam, M. Et. al, "Who Is Responsible for the "Second Disaster"?", Stanford Social Innovation Review <http://ssir.org/articles/entry/who_is_responsible_for_the_second_disaster>, [07/07/2016].

ITU (2013), *Technical Report on Telecommunications and Disaster Mitigation, Focus Group Technical Report.* <https://www.citel.oas.org/en/SiteAssets/About-Citel/Annual-Reports/anual-r10c1_e.pdf> [07/06/2016].

Ley 1341 "por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones." (Colombia) <http://www.mintic.gov.co/portal/604/articles-3707_documento.pdf> [07/06/2016].

Ley de Comercio de Telecomunicaciones de Japón, Telecommunications Business Law- No. 86 <http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/2001TBL.pdf> [07/06/2016].

Ley de Contramedidas a Desastres de Japón (Disaster Countermeasures Basic Act-No. 223, November 15, 1961), <http://www.adrc.asia/documents/law/DisasterCountermeasuresBasicAct.pdf> [07/06/2016].

Ley de Seguridad Pública y del Estado (Ecuador).

Ley de Telecomunicaciones de Chile (Ley 18168). <https://www.leychile.cl/Navegar?idNorma=29591> [07/06/2016].

Ley Orgánica de Telecomunicaciones (Ecuador).

Ministerio de Comunicaciones (2008) *PLAN DE EMERGENCIA Y CONTINGENCIAS DEL SECTOR DE TELECOMUNICACIONES*, Bogotá. <http://www.comunidadandina.org/telec/Plan_telecomunicaciones_colombia.pdf> [07/06/2016].

OEA (1993), *Resolución: AG/RES.1224(XXII-O/93).*

Reglamento a la Ley Orgánica de Telecomunicaciones (Ecuador).

Reglamento para la Prestación de Servicios de Telecomunicaciones y Servicios de Radiodifusión por Suscripción (Ecuador).

Reglamento para llamadas a Servicios de Emergencias (Ecuador).

Secretaría de Gestión de Riesgos (2014) *Resolución No. SGR-038-2014: Manual del Comité de Gestión de Riesgos.*

Secretaría de Gestión de Riesgos-SGR (2014) *Agenda Sectorial de Gestión de Riegos.* <http://biblioteca.gestionderiesgos.gob.ec/files/original/9b1071be15e237ad4eb2f4f678321690.pdf> [07/06/2016].

Secretaría de Gestión de Riesgos-SGR (2016) Informe de situación No.6. http://www.gestionderiesgos.gob.ec/wp-content/uploads/downloads/2016/04/Informe-de-Situaci%C3%B3n-6-01h00.pdf.

UIT (2006a), *Resolución 36: Las Telecomunicaciones/TIC al servicio de la asistencia humanitaria.*<http://www.itu.int/oth/R0B06000017/es> [07/06/2016].

UIT (2006b), *Resolución 136: El uso de las TIC para el seguimiento y la gestión en situaciones de emergencia y de desastre para la alerta temprana, prevención, mitigación y recuperación.* <http://www.itu.int/dms_pub/itu-r/oth/0B/06/R0B060000170001PDFS.pdf > [07/06/2016].

UIT (2010), *Resolución 34: El papel de las telecomunicaciones/TIC en la alerta temprana, mitigación de desastres y ayuda humanitaria.*<https://www.itu.int/dms_pub/itu-s/opb/conf/S-CONF-ACTF-2014-PDF-S.pdf> [07/06/2016].

Protección a la neutralidad de la red en Ecuador

Arturo J. Carrillo
George Washington University

RESUMEN: La regulación de internet debe asegurar que se respete el principio de neutralidad de la red, en el que los proveedores de servicios de internet y los gobiernos tratan el tráfico de datos e información por internet sin discriminación alguna, respetando las obligaciones internacionales del Estado en materia de derechos humanos.

PALABRAS CLAVE: neutralidad de la red, internet, derecho internacional de los derechos humanos, intermediarios de internet.

ABSTRACT: Internet regulation must respect and ensure respect for the principle of net neutrality, which guarantees that all data and information traffic online is treated in a non-discriminatory manner by governments and ISPs, in accordance with the State´s international human rights obligations.

KEYWORDS: net neutrality, internet, international law of human rights, internet intermediaries.

El propósito de este capítulo es revisar las protecciones normativas existentes en Ecuador con respecto a la neutralidad de la red y analizarlas a la luz de los estándares internacionales de derechos humanos aplicables. Recordemos que la neutralidad de la red es el principio según el cual el "tratamiento de los datos y el tráfico de Internet no debe ser objeto de ningún tipo de discriminación en función de factores como dispositivos, contenido, autor, origen y/o destino del material, servicio o aplicación" (Declaración Conjunta, párr. 5 (un)). Las preguntas principales por responder son las siguientes: ¿Hasta qué punto se puede decir que la neutralidad de la red se encuentra adecuadamente protegida en la legislación ecuatoriana? ¿Qué exigen los estándares internacionales de derechos humanos en este sentido y qué debe hacer el Estado ecuatoriano para cumplir sustancialmente con esos estándares? Finalmente, ¿por qué importa tanto que Ecuador (y los demás países del mundo) cumpla con estas obligaciones para garantizar adecuadamente la neutralidad de la red?

Si bien el objetivo central de este texto es analizar el marco legal ecuatoriano en lo que concierne a la neutralidad de la red, corresponde esbozar, primero, los parámetros pertinentes establecidos por el derecho internacional de los derechos humanos. Esto significa revisar las normas relevantes del Sistema interamericano de protección de los derechos humanos, así como el Sistema universal de la organización de Naciones Unidas. En particular, se hará énfasis en el Artículo 13 de la Convención Americana sobre Derechos Humanos y en el Artículo 19 del Pacto Internacional de Derechos Civiles y Políticos de Naciones Unidas que regulan la libertad de expresión (CADH 1969; PIDCP, 1966). Una vez identificados los estándares internacionales pertinentes, aplicables al Ecuador debido a su condición de Estado Parte en ambos regímenes convencionales, se podrá estudiar cuáles son las leyes y normas del orden jurídico nacional que se dirigen hacia el principio de la neutralidad de la red. Un análisis técnico de la normativa nacional, evaluada a la luz de los estándares internacionales señalados, permitirá realizar, a manera de conclusión, una reflexión sobre el deficiente estado de cumplimiento del Ecuador en cuanto a sus obligaciones internacionales en la materia.

No está demás recordar antes de comenzar que los tratados de derechos humanos ratificados por Ecuador, así como la Convención Americana y el Pacto Internacional, gozan de un rango privilegiado en la jerarquía constitucional de normas. Así, el Artículo 424 de la Constitución de Ecuador de 2008 reza que la "Constitución y los tratados internacionales de derechos humanos ratificados por el Estado que reconozcan derechos más favorables a los contenidos en la Constitución, prevalecerán sobre cualquier otra norma jurídica o acto del poder público". En este mismo sentido, el Artículo 425 que prescribe el orden jerárquico de aplicación de normas coloca a "los tratados y convenios internacionales" por encima de "las leyes orgánicas; las leyes ordinarias; las normas regionales y las ordenanzas distritales; los decretos y reglamentos; las ordenanzas; los acuerdos y las resoluciones; y los demás

actos y decisiones de los poderes públicos". Cualquier conflicto entre normas se resolverá "mediante la aplicación de la norma jerárquica superior" (Constitución de Ecuador, Art. 425). Este marco constitucional tiene implicaciones importantes para el posterior análisis del orden jurídico interno y la neutralidad de la red con el que concluye el capítulo.

1. Sistema Interamericano de Protección de los Derechos Humanos

Tratándose de la neutralidad de la red, el Sistema interamericano exige a los Estados Partes de la Convención Americana sobre Derechos Humanos adoptar una protección amplia y robusta de ese principio. En 2013, la Relatora Especial de la OEA para la Libertad de Expresión, Catalina Botero ("Relator Especial de la OEA"), afirmó que la Convención Americana, Artículo 13 que regula la libertad de expresión "se aplica plenamente a las comunicaciones, las ideas y la información distribuida a través de Internet" (Relator Especial de la OEA, 2014, párr. 2). Al interpretar la Convención Americana, el Relator Especial observó que el respeto de neutralidad de la red "es una condición necesaria para el ejercicio de la libertad de expresión en Internet con arreglo a los términos del artículo 13" (Relator Especial de la OEA, 2014, párr. 25). Esto se debe a que "la neutralidad se desprende del diseño original de Internet [...] es fundamental para garantizar la pluralidad y diversidad de los flujos de información" (Relator Especial de la OEA de 2014, párrs. 27-28). Estas declaraciones significan que el Sistema interamericano de derechos humanos va más allá, incluso que su homólogo de la ONU, en lo que se refiere a tratar y proteger *expresamente* los principios de neutralidad de la red en varios aspectos importantes, como veremos a continuación.

El Artículo 13 de la Convención Americana, aunque similar al Artículo 19 del PIDCP en la mayoría de los aspectos claves, se diferencia positivamente en otros que vale la pena resaltar. Al igual que su contraparte de la ONU, el Artículo 13 protege la libertad de expresión, en todas sus dimensiones (párrafo 1) y establece un régimen de excepciones que funciona de manera casi idéntica a la versión del Artículo 19 (párrafo 2). Pero, también adopta una prohibición expresa de "censura previa" (párrafo 2), así como sobre las restricciones "por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres o aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones"(artículo 13.3). En este mismo orden de ideas, los artículos de la Convención Americana que prohíben la discriminación en la implementación y mantenimiento de los derechos consagrados por el tratado, reconocen expresamente distinciones ilegales hechas sobre la base de una "posición económica" (artículos 1.1 y 24). Esto también distingue positivamente a

la Convención en contraste con su contraparte, el PIDCP, por lo menos en lo que se refiere a su versión original en inglés.[1]

Resulta difícil exagerar la importancia de estas protecciones normativas para la neutralidad de la red y la libertad de expresión en las Américas. Entre las consecuencias jurídicas primarias, catalogadas por el Relator Especial de la OEA, se hace énfasis en que los Estados parte de la Convención Americana deben:

> Garantizar la aplicación efectiva del principio de neutralidad de la red a través de una "legislación adecuada" (Relator Especial de la OEA, 2014, párr. 26) que debe ser "resultado del diálogo de todos los actores y mantenga las características básicas del entorno original, potenciando su capacidad democratizadora e impulsando el acceso universal y sin discriminación" (párr. 11);
>
> Asegurar que "la libertad de acceso y elección de los usuarios de utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal por medio de Internet no esté condicionada, direccionada o restringida, por medio de bloqueo, filtración, o interferencia" (Relator Especial de la OEA de 2014, párrafo 25);
>
> Garantizar que cualquier restricción a neutralidad de la red y la libertad de expresión "se encuentre establecida por medio de leyes en sentido formal y material y que dichas leyes sean claras y precisas" (Relator Especial de la OEA, 2014, párr. 58). Estas restricciones deben igualmente corresponder a un objetivo legítimo e imperativo del Estado como aquellos enumerados en el párrafo 2 del artículo 13, que incluye el respeto por los derechos de los demás, así como respetar los principios básicos de necesidad, proporcionalidad y el debido proceso (párr. 55);
>
> Prohibir por incompatibles con la Convención Americana "las restricciones sustantivas definidas en disposiciones administrativas o las regulaciones amplias o ambiguas que no generan certeza sobre el ámbito del derecho protegido y cuya interpretación puede dar lugar a decisiones arbitrarias que comprometan de forma ilegítima el derecho a la libertad de expresión." (Relator Especial de la OEA, 2014, párr. 58);
>
> Proteger el pluralismo en línea al " asegurar que no se introduzcan en Internet cambios que tengan como consecuencia la reducción de voces y

1 La versión en inglés del PIDCP señala como base prohibida una centrada en "*property,*" lo que significa "[l]o que se posee, especialmente si se trata de un bien inmueble", según el diccionario del El Mundo de España (http://www.elmundo.es/diccionarios/). Pero la versión oficial al español del PIDCP traduce "property" como "posición económica". Ése sería un error, ya que "posición económica" es otro concepto que va más allá de los bienes poseídos. En cambio, ambas versiones de la Convención Americana convergen en hablar de "economic status", por un lado, y "posición económica", por el otro, que sí son términos homólogos.

contenidos. Las políticas públicas sobre la materia deben proteger la naturaleza multidireccional de Internet y promover las plataformas que permitan la búsqueda y difusión de informaciones e ideas de toda índole, sin consideración de fronteras, en los términos del artículo 13 de la Convención Americana” (Relator Especial de la OEA, 2014, párr. 19);

Adoptar las medidas necesarias “para prevenir o remediar restricciones ilegítimas al acceso a Internet por parte de particulares y empresas, como las políticas que atentan contra la neutralidad de la red o la prevalencia de prácticas anticompetitivas” (Relator Especial de la OEA, 2014, párr. 51);

Respetar y garantizar no solo los derechos de libertad de expresión de los individuos, sino también de la sociedad. Esta “doble dimensión” inherente al derecho de libertad de expresión consiste, por un lado, en “el derecho a comunicar a otros el propio punto de vista y las informaciones u opiniones que se quieran”; por el otro, “el derecho de todos a recibir y conocer tales puntos de vista, informaciones, opiniones, relatos y noticias, libremente y sin interferencias que las distorsionen u obstaculicen”. (Relator Especial de la OEA, 2014, párr. 35).

2. Sistema de Naciones Unidas para los derechos humanos

En América Latina, este sistema se conoce comúnmente como el sistema de derechos humanos “universal”. El Pacto Internacional de Derechos Civiles y Políticos (en adelante “PIDCP” o “Pacto”) cuenta con 168 Estados Partes, entre ellos Ecuador, que abarcan más del 85% de la población mundial (Oficina del Alto Comisionado para los Derechos Humanos). Sin duda, sus principios básicos se aplican a casi todos los países del planeta (Oficina del Alto Comisionado de Derechos Humanos, 2009)[2]. Por lo tanto, cuando se habla de los derechos humanos en línea, el marco de la ONU es un referente necesario. Esto se debe no solo a su cobertura casi universal, sino también a la importancia que esta organización ha adquirido por los expertos y autoridades que forman parte de las Naciones Unidas y que contribuyen a su desarrollo.

La neutralidad de la red es, hoy por hoy, una norma consolidada en el marco jurídico de Naciones Unidas, debido al papel fundamental que desempeña para hacer cumplir la protección de la libertad de expresión y la no discriminación en la sociedad contemporánea. El Artículo 19 del PIDCP afirma el derecho “de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro medio de su elección […]”. La libertad de expresión goza de aceptación casi

2 La Declaración Universal de Derechos Humanos es considerada una fuente de derecho internacional consuetudinario, para normas centrales como la libertad de expresión, que se aplica a todos los Estados Miembros de la ONU sin importar su ratificación al PIDCP.

universal en todo el mundo, entre otras cosas porque es un facilitador de varios otros derechos humanos fundamentales. Estos incluyen no solo los principios al derecho de opinión y creencias religiosas sin interferencias, sino también varios otros derechos. Algunos ejemplos son el derecho a la educación, el derecho a la libertad de asociación y reunión, el derecho a la plena participación en la vida social, cultural y política y el derecho al desarrollo social y económico (Relator Especial de la ONU de 2011, p. 18).

Tradicionalmente, la libertad de expresión ha sido dividida en varios elementos constitutivos, dentro de los cuales se ha incluido el derecho a difundir información y a expresar ideas, así como el derecho de buscar, solicitar y recibir información (CCPR Observación general 34, párr. 10, 5)[3]. Es importante destacar, asimismo, el deber de los Estados de promover y proteger la pluralidad de los medios de comunicación:

> El Estado no debe ejercer un control monopolístico sobre los medios de comunicación, sino que ha de promover la pluralidad de estos. Por consiguiente, los Estados partes deberían adoptar medidas adecuadas, en forma compatible con el Pacto, para impedir un excesivo predominio o concentración de los medios de comunicación por grupos mediáticos bajo control privado, en situaciones monopolísticas que pueden menoscabar la diversidad de fuentes y opiniones" (CCPR Observación General 34, párr. 40)

Con el auge de las comunicaciones electrónicas, este marco normativo ha evolucionado para dar cabida a la expresión y recepción de información a través de internet. En el derecho internacional de los derechos humanos se reitera que los derechos que comprenden la libertad de expresión se aplicarán a todos los "modos basados en el Internet de la comunicación" (CCPR Observación general 34, párr. 12). Expertos de las Naciones Unidas y otros sistemas de derechos humanos han reconocido explícitamente que "el tratamiento de los datos y el tráfico de Internet no debe ser objeto de ningún tipo de discriminación en función de factores como dispositivos, contenido, autor, origen y/o destino del material, servicio o aplicación. "(Declaración Conjunta, párr. 5 (un)). Esta, por supuesto, es la definición técnica de neutralidad de la red que ya se señaló.

Según las Naciones Unidas, proteger adecuadamente a la neutralidad de la red significa que:

> "toda limitación al funcionamiento de los sitios web, los *blogs* u otros sistemas de difusión de información en Internet, electrónicos o similares, incluidos los sistemas de apoyo a estas comunicaciones, como los proveedores de servicios de Internet o los motores de búsqueda, solo serán admisibles en la medida en que sean compatibles con el párrafo 3 [del Artículo

3 Los otros elementos son los derechos de los medios de comunicación y el acceso a la información de las entidades públicas.

> 19 del PIDCP]. Las restricciones permisibles se deben referir en general a un contenido concreto; las prohibiciones genéricas del funcionamiento de ciertos sitios y sistemas no son compatibles con el párrafo 3 [del artículo 19] "(CCPR Observación general 34, párr. 43).

Para completar la panoplia de la libertad de expresión de los elementos relacionados con la neutralidad de la red, tomamos en cuenta el derecho a acceder a internet e información en línea o la conectividad. En pocas palabras, "los Estados tienen la obligación de promover el acceso universal a Internet para garantizar el disfrute efectivo del derecho a la libertad de expresión" (Relator Especial de la ONU et. Al. 2011, párr. 6 (a)). Esta obligación positiva significa que los Estados, para cumplir con su deber de respetar y garantizar el derecho a la libertad de expresión, deben garantizar que todas las personas dentro de su territorio tengan acceso a "los medios necesarios para ejercer este derecho, que [hoy] incluye Internet "(Relator Especial de la ONU de 2011, párr. 61). En consecuencia, el Comité de Derechos Humanos de la ONU (conocido por sus siglas en inglés como CCPR) ha dictaminado que los Estados "deberían tomar todas las medidas necesarias para fomentar la independencia de [...] nuevos medios y asegurar el acceso a los mismos de los particulares" (CCPR Observación general 34, párr. 15). La conectividad es, por lo tanto, "esencial" para la realización de la libertad de expresión (Relator Especial de la ONU de 2011, párr. 61).

La neutralidad de la red es, en el fondo, una norma de no discriminación. En términos de derechos humanos, se trata del derecho de toda persona de solicitar, recibir, transmitir o difundir cualquier información en línea sin discriminación alguna (Carrillo, 2016). En este punto, el Pacto establece en su Artículo 2 que los Estados Partes tienen la obligación de "respetar y garantizar a todos los individuos que se encuentren dentro de [su] territorio y estén sujetos a [su] jurisdicción los derechos [humanos] reconocidos [...], sin distinción alguna de raza, color, sexo, idioma, religión, opiniones políticas u otras, origen nacional o social, posición económica [*property*], nacimiento o cualquier otra condición". Definir qué cuenta como "cualquier otra condición" a efectos de la determinación de las distinciones adicionales que podrían llevar a un aspecto negativo o a la discriminación positiva es una pregunta abierta. Lo que es seguro es que el derecho internacional de derechos humanos reconoce distinciones basadas en condiciones económicas y evalúa si su propósito es el efecto de anular o menoscabar el ejercicio o el disfrute de otros derechos humanos (*Haraldsson y Sveinsson v. Islandia*, 2007). Esta es la razón por la que las restricciones propuestas a la neutralidad de la red como el *zero-rating*, que ofrece un acceso preferencial gratuito a ciertos servicios o aplicaciones en internet, deben ser examinadas de cerca para evaluar su impacto en el ejercicio de la libertad de expresión.

En la medida en que la neutralidad de la red se entiende como un principio de no discriminación aplicado a los derechos de los usuarios para solicitar, reci-

bir y difundir datos o información en línea, se integra orgánicamente al núcleo de normas de no discriminación del derecho internacional de los derechos humanos. Pero no toda discriminación es ilegal *per se*. El derecho internacional distingue entre discriminación negativa y positiva. El "principio de la igualdad exige algunas veces a los Estados Partes adoptar disposiciones positivas para reducir o eliminar las condiciones que originan o facilitan que se perpetúe la discriminación prohibida [por el derecho internacional]" (CCPR, Comentario General 18, párr. 10). Por esta razón, "no toda diferenciación de trato constituirá una discriminación, si los criterios para tal diferenciación son razonables y objetivos y lo que se persigue es lograr un propósito legítimo en virtud [de las leyes]" (CCPR, Comentario General 18, párr. 13). En otras palabras, la discriminación positiva o afirmativa puede ser una medida excepcional que mejora o aumenta el ejercicio general y el disfrute de los derechos humanos y que produce un beneficio neto.

El *zero-rating*, por ejemplo, actúa como una restricción discriminatoria a la neutralidad de la red, principio que, como hemos visto, es hoy una norma integral a los derechos a la libertad de expresión y la no discriminación. En virtud del derecho internacional de los derechos humanos, hay algunas circunstancias en las que tal restricción podría ser permitida (Carrillo, 2016). Esto se debe a que las normas de derechos humanos y a la libertad de expresión, en particular, no son absolutas. Las leyes sobre difamación son un ejemplo clásico de los límites estrictos impuestos a la libertad de expresión, con el fin de proteger los derechos de los demás (OHCHR, 2011, párr. 47)[4]. Y, al igual que "la diferenciación legítima" a favor de los grupos históricamente desfavorecidos puede alcanzar, de manera efectiva, los objetivos de la no discriminación, (CCPR, Observación General 18, párr. 10), también pueden los derechos alrededor de la libertad de expresión de algunos (para impartir o recibir información libremente) ser reducidos mediante la discriminación positiva (*zero-rating*) destinada a promover los derechos de libertad de expresión de los demás (a la conectividad) (CCPR Observación general 34, párr.. 28;. Carrillo, 2016). La cuestión tiene que ver, entonces, con aspectos como si tal discriminación "legítima" es necesaria y proporcionada cuando existe un objetivo imperativo de Estado reconocido por el DIDH que se busca alcanzar.

Del mismo modo, el Artículo 19.3 del PIDCP permite expresamente ciertas restricciones al derecho a la libertad de expresión cuando sea necesario "asegurar el respeto a los derechos o a la reputación de los demás" o para avanzar "la protección de la seguridad nacional, el orden público o la salud o la moral públicas". Estos son, en términos generales, los únicos objetivos que pueden ser invocados por los Estados que tratan de imponer límites a los derechos humanos fundamentales, incluyendo la libertad de expresión (Relator Especial de las Naciones Unidas, 2012,

4 Otro buen ejemplo es PIDCP art. 20, que enumera de forma explícita una serie de formas ofensivas de expresión que debe quedar restringida por los Estados con el fin de cumplir con sus obligaciones en virtud del tratado. ("1. Toda propaganda en favor de la guerra estará prohibida por la ley. 2) Toda apología del odio nacional, racial o religioso que constituya incitación a la discriminación, la hostilidad o la violencia estará prohibida por la ley.")

párr. 28). Además de perseguir un fin legítimo, un Estado que pretende limitar la libertad de expresión (u otros derechos humanos básicos), debe asegurarse de que las medidas para hacerlo estén "fijadas por la ley" y que sean "necesarias" para cumplir con el objetivo declarado, así como "proporcionales" (CCPR Observación general 34, párrafos 24-26, 33-34;. PIDCP, 1966, Artículo 19.3). El funcionamiento del régimen de excepciones en virtud del Pacto, sin embargo, no es un cheque en blanco: "Cuando un Estado impone restricciones al ejercicio de la libertad de expresión, éstas no pueden poner en peligro el derecho propiamente dicho" (CCPR Observación general 34, párr. 21). En otras palabras, las excepciones deben ser excepcionales, y no pueden convertirse en la regla.

Suponiendo que el fin de un Estado es lograr uno de los objetivos legítimos reconocidos por el derecho internacional, cualquier restricción a la libertad de expresión propuesta como medio para avanzar hacia dicho objetivo no solo debe estar prevista por ley, sino también debe ser necesaria y proporcional. Eso tiene como propósito hacer muy difícil que se reconozca más que un pequeño conjunto de posibles medidas estrechamente definidas (CCPR Observación general 34, nota 275, párr. 35). En términos generales, estas restricciones deben ser promulgadas por ley formal a través de un proceso político transparente y participativo (Relator Especial de la ONU, 2012). En cualquier caso, este tipo de leyes "deben ser formuladas con precisión suficiente para que una persona pueda regular su conducta en consecuencia;" además, deben ser accesibles al público (CCPR Observación general 34, nota 275 párr. 35). Al ser "necesarios" los límites legalmente promulgados deben estar "directamente relacionados con la necesidad específica de la que dependen", es decir, deben ser eficaces para hacer lo que están destinados a hacer (CCPR Observación general 34, párr. 22). Una restricción no es indispensable y, por lo tanto, "viola el criterio de necesidad [,] si la protección podría lograrse de otras maneras que no restringen la libertad de expresión" (OHCHR de 2011, párr. 33). Por último, una medida tomada por un Estado para limitar la expresión, aunque legítima y necesaria, no puede ser "demasiado amplia" (CCPR Observación general 34, párr. 34). Medidas proporcionadas son las "adecuadas para desempeñar su función protectora" y "la menos intrusiva [...] entre aquellas [disponibles]" (CCPR Observación general 34, párr. 34).

3. La protección a la neutralidad de la red en Ecuador

La neutralidad de la red en Ecuador se encuentra codificada por la Ley Orgánica de Telecomunicaciones promulgada en 2015 (en adelante "LOT"). Este principio se menciona dentro de los objetivos (Art. 3) y principios (Art. 4 y 66) de la Ley. Además, el numeral 18 del Artículo 22 dictamina que los abonados, clientes y usuarios de servicios de telecomunicaciones tienen derecho a: "[…] acceder a cualquier aplicación o servicio permitido disponible en la red de internet." A continuación, se afirma que:

> los prestadores no podrán limitar, bloquear, interferir, discriminar, entorpecer ni restringir el derecho de sus usuarios o abonados a utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación, desarrollo o servicio legal a través de Internet o en general de sus redes u otras tecnologías de la información y las comunicaciones.

Sin embargo, según el mismo numeral, este deber "puede ser excusado por [el usuario o] por disposición de autoridad competente"; es decir, en cualquier circunstancia, la autoridad (por ejemplo, un juez o el Ministro de Telecomunicaciones y de la Sociedad) puede según su propio criterio restringir ese derecho.[5]

Asimismo, el Artículo 64 de la LOT, que habla de la Reglas Aplicables a las tarifas y precios, señala que "los prestadores de los servicios podrán establecer planes tarifarios constituidos (…) por uno o varios productos de un servicio". Tomado en conjunto con lo dispuesto a manera de excepción en el numeral 18 del Artículo 22, este régimen abre la puerta a que las empresas de telefonía e internet móvil puedan legalmente diferenciar entre las aplicaciones y los servicios que ofrecen, lo que violaría el principio de la neutralidad de la red (Delgado, 2015). Es curioso el hecho de que, si bien la LOT elevó al rango de ley ese principio que antes se veía codificada por reglamento, también cambió su enfoque para permitir que las empresas de telefonía pudieran ofrecer planes y servicios diferenciados, lo que antes estaba expresamente prohibido en la regla correspondiente del reglamento (Delgado, 2015).

Este giro en el marco jurídico nacional con respecto a la neutralidad de la red ha generado ya efectos. Por ejemplo, Movistar y Claro, entre otros, ofrecen hoy uso ilimitado de algunos servicios y ciertas aplicaciones junto con sus planes de datos limitados. Así, al suscribirse a un plan de datos con capacidad determinada de Claro, el usuario puede, sin costo adicional, tener uso ilimitado de mensajería instantánea por WhatsApp, Google y Yahoo!. Si el plan de datos es de Movistar, el usuario puede gozar de acceso sin restricción a WhatsApp y Facebook (Fundación Karisma, pág. 48). La práctica de circunscribir el ámbito protector de la neutralidad de la red por medio de ofertas comerciales que incluyen servicios gratuitos excluidos de los planes de datos debilita la efectividad de dicha norma y amenaza con socavarla por completo, si no existe una regulación concienzuda por parte de las autoridades competentes.

Ya hay un ejemplo de esto en Ecuador. Hubo una demanda contra Movistar y Claro precisamente por ofrecer el servicio de mensajería instantánea de WhatsApp gratis e ilimitado con sus planes de datos limitados. Resulta que dichas ofertas no incluían la funcionalidad de llamadas de voz que normalmente integra la aplica-

5 Esta observación se la debo a Juan Carlos Solines, Taller Preparatorio, Universidad San Francisco de Quito, 24 de junio de 2016.

ción WhatsApp. Sobre la situación, el Ministro de Telecomunicaciones y de la Sociedad de la Información (MINTEL) declaró que la práctica de no incluir la función de hacer llamadas en los paquetes con *zero-rating* de WhatsApp iba en contra del principio de neutralidad de la red establecido en la LOT y anunció que el organismo regulador, Arcotel, investigará los hechos (Karisma, 2016, p. 47).

Así las cosas, corresponde ahora ver qué dice el proyecto de ley del Código Orgánico de la Economía Social de los Conocimientos, mejor conocido como el "Código de 'Ingenios'". Según el texto actual del proyecto de ley, esta norma se pronunciaría acerca de la neutralidad de la red de la siguiente manera:

> "El Estado generará las condiciones necesarias para garantizar progresivamente la universalización del acceso a las tecnologías de la información y comunicación, priorizando el uso de tecnologías libres, bajo los principios de: soberanía tecnológica, seguridad, neutralidad de la red, acceso libre y sin restricciones a la información y precautelando la privacidad" (énfasis agregado).

Se entiende que la definición operante de este principio en el Código propuesto tiene que ser la de la Ley Orgánica de Telecomunicaciones.

4. Análisis

La primera pregunta para responder es si la neutralidad de la red se encuentra adecuadamente protegida por la legislación ecuatoriana. Si bien la definición de este principio que codifica la Ley Orgánica de Telecomunicaciones concuerda con los parámetros reconocidos por los expertos internacionales en derechos humanos de la OEA y la ONU, entre otros, las excepciones, igualmente codificadas por la LOT en los Artículos 22 y 64, generan fuertes dudas al respecto, por varias razones. En primer lugar, el derecho internacional de los derechos humanos (DIDH) exige que cualquier legislación que afecte el goce de la libertad de expresión debe ser resultado de un proceso político transparente, con una participación amplia de sociedad civil y "diálogo de todos los actores" (Relator Especial de la OEA, 2014, párr. 26; Relator Especial de la ONU, 2011). Pero este no ha sido el caso con respecto a la legislación ecuatoriana encaminada a regular la neutralidad de la red. Como en su momento se señaló, la Asamblea Nacional de Ecuador aprobó la nueva Ley Orgánica de Telecomunicaciones tras "un debate bastante breve y con escasa participación de la ciudadanía" (Delgado, 2015).

En segundo lugar, si el gobierno ecuatoriano quiere restringir la neutralidad de la red, o permitir restricciones por parte de varios actores privados, debe hacerlo mediante leyes formales que "sean claras y precisas", para permitir que toda persona afectada pueda percibir su alcance (Relator Especial de la OEA, 2014, párr. 26). Así, "serían incompatibles con la Convención Americana [y el Pacto Internacional] las restricciones [...] amplias o ambiguas que no generan certeza sobre el ámbito

del derecho protegido y cuya interpretación puede dar lugar a decisiones arbitrarias que comprometan de forma ilegítima el derecho a la libertad de expresión." (Relator Especial de la OEA, 2014, párr. 58; Relator Especial de la ONU, 2011). Entre otras deficiencias, las excepciones a la neutralidad de la red promulgadas por la LOT en el numeral 18 del Artículo 22 son excesivamente amplias y ambiguas. Por un lado, no define cuáles serían las autoridades competentes para excusar el deber de respetar el principio de neutralidad de la red. Por el otro, el numeral 18 no precisa cuándo o cómo dicha "autoridad competente" puede autorizar o desestimar limitaciones a esta norma en la práctica. El resultado es "un cheque en blanco" para que una serie de autoridades pueda según su propio criterio circunscribir la neutralidad de la red. Tampoco está claro cuáles serían los recursos disponibles según la ley para personas o entidades perjudicadas por las decisiones de estas autoridades. Todas estas imprecisiones abren la puerta a la arbitrariedad.

Lo mismo se puede decir del Artículo 64 de la LOT que permite a los prestadores de servicios móviles ofrecer planes con servicios diferenciados, incluyendo por medio del *zero-rating*, sin imponer parámetros algunos a esa práctica potencialmente nociva para la neutralidad de la red. En este sentido, el Estado debe asegurar que existan las medidas necesarias "para prevenir o remediar restricciones ilegítimas al acceso a Internet por parte de [...] empresas, [tales] como las políticas que atentan contra la neutralidad de la red o la prevalencia de prácticas anticompetitivas" (Relator Especial de la OEA, 2014, párr. 51: Relator Especial de la ONU, 2011).

El caso arriba reseñado de WhatsApp sugiere que en algunos escenarios el riesgo podría ser menos en la medida que MINTEL cumpla de manera constructiva con su papel regulador. Pero como la LOT no ofrece una definición íntegra de neutralidad de la red, ni fija las pautas rectoras para su implementación con precisión, no hay garantía alguna de que las empresas afectadas no abusen de su competencia, o de que las autoridades competentes vayan a actuar con la diligencia debida para evitar y remediar arbitrariedades. Como bien observa Andrés Delgado, si bien el Ministerio obró positivamente en el caso de WhatsApp, no hay garantía de que lo siga haciendo porque el cumplimiento de la Ley "es vulnerable a los cambios en la política de MINTEL" (Delgado, 2015). El papel del regulador entonces es clave, entre otras razones, porque modificar la LOT no parece ser una opción viable a corto o mediano plazo (Delgado, 2015).

En tercer lugar, si las autoridades ecuatorianas permiten limitaciones al principio de la neutralidad de la red como es el *zero-rating*, dicha autorización debe cumplir con todos los requisitos del régimen de excepciones a la libertad de expresión, empezando por con contar con un objetivo "imperativo" de Estado (CCPR, Observación general 34, párrs. 28, 29; Relator Especial de la OEA, 2014). Los objetivos reconocidos expresamente por el DIDH como legítimos en este sentido son la necesidad de respetar los derechos o la reputación de los demás, así como asegurar la protección de la seguridad nacional, el orden público, la salud o la moral públicas (CCPR, Observación general 34, párrs. 28, 29; Relator Especial de la OEA, 2014).

Lo más probable es que una política pública que permita la diferenciación entre planes de acceso a internet, por razones puramente *comerciales*, no cumpla con los requisitos del DIDH de contar con una de estas motivaciones reconocidas como "legítimas". Este parece ser el caso de Ecuador en la actualidad. En cambio, una política de Estado que busque promover mayores índices de conectividad entre una población que no goza de un acceso a internet en su gran mayoría, ni tampoco de los beneficios que ese acceso conllevaría, sí podría en principio justificarse a la luz del DIDH (Carrillo, 2016).

¿Por qué resulta tan importante velar por la adecuada codificación e implementación de la neutralidad de la red en Ecuador? Porque la Convención Americana y el Pacto Internacional imponen a los Estados Partes como Ecuador la obligación categórica de adoptar las medidas necesarias para hacer efectivo el derecho a la libertad de expresión, sin discriminación alguna. Como se ha visto, este deber acarrea, a su vez, la obligación de adoptar medidas legislativas y de otra índole y encaminarlas para hacer efectiva la neutralidad de la red. Dicho de otra manera, sin una neutralidad de la red bien codificada y protegida, no puede haber libertad de expresión en internet y el Estado ecuatoriano se expondría a una responsabilidad internacional en el DIDH por violaciones de ese principio.

Para terminar, pongo como ejemplo a Colombia, país en el que se ha promulgado una legislación que codifica el principio de la neutralidad de la red en términos similares a los de Ecuador. En 2011, Colombia promulgó la Ley 1450 en la que se consagró un concepto de neutralidad de la red que prohíbe expresamente el bloquear, interferir, discriminar o restringir los derechos de los usuarios de internet para acceder, enviar, recibir o publicar cualquier contenido, aplicación o servicio en línea (Fundación Karisma, 2016, p.37). Al mismo tiempo, la Ley 1450 establece que los proveedores de servicios de internet pueden "hacer ofertas en función de las necesidades de los sectores del mercado o de los suscriptores de los proveedores de acuerdo a su consumo y perfiles de usuario, *que no ha de interpretarse como una discriminación*" (Fundación Karisma, 2016, p. 37) (énfasis agregado). El reglamento de aplicación de la Ley 1450 deja claro que esta excepción a la definición de discriminación, para efectos de neutralidad de la red, autoriza la oferta de planes que proporcionan un acceso restringido a internet, por medio de ciertos tipos "genéricos" de los servicios, contenidos o aplicaciones, siempre que los proveedores de servicios ofrezcan planes con acceso ilimitado a internet, al lado de aquellos que tiendan a limitarlo (Fundación Karisma, 2016, p. 37). Y, de hecho, en Colombia actualmente se ofrece una variedad de planes con *zero-rating* de servicios como los de WhatsApp y Facebook (Fundación Karisma, 2016, págs. 39-40).

La Fundación Karisma, una ONG colombiana que aboga a favor de los derechos digitales, ha expresado su preocupación por esta situación. Entre otros problemas, el concepto de discriminación adoptado por la Ley 1450 contradice francamente la definición de neutralidad de la red en la misma ley (y en el DIDH), de tal manera

que, junto con el reglamento citado, la Ley 1450 amenaza con hacerle "burla" al mismo principio que pretende consagrar (Fundación Karisma, 2016, p.37). También es preciso recordar que Colombia, similar a lo que sucede en Ecuador, es un Estado "monista", donde los tratados de derechos humanos, una vez ratificados, entran a formar parte de un "bloque constitucional" de normas que pueden ser invocadas directamente ante los tribunales colombianos (Constitución de Colombia, art. 93). Así las cosas, y teniendo en cuenta el marco jurídico internacional reseñado en las primeras dos partes de este capítulo, no es difícil prever cómo la situación colombiana respecto de las normas sobre neutralidad de la red y la práctica de *zero-rating* podrían fácilmente dar lugar a demandas legales contra la Ley 1450, por transgredir las obligaciones del Estado en materia de derechos humanos. Dichas acciones podrían incluso llevar ante instancias internacionales de derechos humanos una vez se agoten los recursos internos.

Eventualmente, lo mismo podría decirse de Ecuador. Los términos pertinentes de la LOT y su implementación dan pie a dudas similares a las que surgen en Colombia frente a la Ley 1450 y su reglamentación. La responsabilidad de asegurar que dichas normas se cumplan con arreglo a las obligaciones internacionales del Estado de garantizar la libertad de expresión y la no discriminación recae, en primer lugar, sobre los funcionarios que vigilan su implementación y cumplimiento. Pero es también desde la sociedad civil que la importancia del tema debe defenderse, sobre todo ante un eventual incumplimiento de sus obligaciones por las autoridades nacionales.

Bibliografía:

Asamblea General de la ONU, Pacto Internacional de Derechos Civiles y Políticos (PIDCP), Dic. 16, 1966, Series sobre tratados, vol. 999. Tomado desde https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en.

Botero, C. (2014). Relatora Especial de la OEA para la Libertad de Expresión y el Internet. Tomado desde http://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_Internet_ENG%20_WEB.pdf.

Cámara de Diputados. (1917). Constitución Política de los Estados Unidos Mexicanos. Últimas reformas publicadas en diciembre 27, 2013. Tomado desde http://www.diputados.gob.mx/LeyesBiblio/htm/1.htm.

Carrillo, A.J. (2016). Having Your Cake and Eating it Too? Zero-Rating, Net Neutrality and International Law. Tomado desde http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2746447.

Carrillo, A.J., & Nunziato, D.C. (2015). The Price of Paid Prioritization: International Law Consequences of the Failure to Protect Net Neutrality by the United

States. Georgetown Journal of International Affairs, Volumen: International Engagement on Cyber V: Securing Critical Infrastructure.

Comité de Derechos Humanos de Naciones Unidas. Comentario General, No. 18, 10 Nov. 1989. Tomado desde http://hrlibrary.umn.edu/gencomm/hrcom18.htm.

Comité de Derechos Humanos de Naciones Unidas. Comentario General, No. 34, 12 Sep. 2011 Documento Naciones Unidas CCPR/C/GC/34.

Constitución Política de Colombia. (1991).

Constitución de la República de Ecuador (2008).

Delgado, Andrés, La neutralidad de la red se debilita en Ecuador, Derechos No. 28, 31 de enero de 2015. Tomado desde http://www.digitalrightslac.net/es/la-neutralidad-de-la-red-se-debilita-en-ecuador/

Fundación Karisma. (2016). ¿Cómo se Contrata en Latinoamérica el acceso a internet? ¿Qué tiene que ver esto con la neutralidad de la red? Tomado desde https://karisma.org.co/ofertas-de-acceso-a-internet-en-america-latina/.

Haraldsson y Sveinsson v. Iceland. Comunicado No. 1306/2004, Documento Naciones Unidas. A/63/40, para. 10.3 (2007). Tomado desde http://www.worldcourts.com/hrc/eng/decisions/2007.10.24_Haraldsson_v_Iceland.htm.

La Rue, F. (2012).Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión. A/HRC/23/40.

Ley Orgánica de Telecomunicaciones (2015).

McCarthy, K. (2016, Enero 13). Council of Europe Gets Tough on Net Neutrality. Tomado desde http://www.theregister.co.uk/2016/01/13/council_of_europe_net_neutrality_guidelines/.

Oficina del Alto Comisionado para Derechos Humanos. (2009). Digital Record of the UDHR. Tomado desde http://www.ohchr.org/EN/NEWSEVENTS/Pages/DigitalrecordoftheUDHR.aspx.

Oficina del Alto Comisionado para Derechos Humanos. Status of Ratifications, Reservations and Declarations. Tomado desde http://indicators.ohchr.org.

Organización de los Estados Americanos. (1969). Convención Americana de Derechos Humanos (CADH). Serie sobre tratados, No. 36. San José: Organización de los Estados Americanos. Tomada desde http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=62&lID=2 .

Proyecto de Ley: Código Orgánico de la Economía Social de los Conocimientos ("Ley de Ingenios") 2016.

Relator Especial para la Libertad de Expresión y el Internet. (2011). Rep. on the Promotion and Protection of the Right to Freedom of Opinion and Expression. Documento de Naciones Unidas. A/66/290, 18, para. 61. Tomado desde http://www.ohchr.org/documents/issues/opinion/a.66.290.pdf.

Relatoría Especial para la libertad de expresión de las Naciones Unidas, Relator de las Naciones Unidas para la Libertad de Pensamiento y Expresión, Representante para la libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE) y Relator de la Comisión Africana de Derechos Humanos y de los Pueblos(2011). Declaración Conjunta sobre Libertad de Expresión e Internet. Tomado desde http://www.osce.org/fom/78309.

Regulación de Propiedad Intelectual en Internet: La Paradoja del Siglo XXI

Sophia Espinosa Coloma
Universidad San Francisco de Quito

RESUMEN: Existe una estrecha interrelación entre la Sociedad de la Información y la economía del conocimiento que debe ser revisada. En este marco, existen maneras distintas de adaptar la norma existente a derechos de autor y propiedad intelectual para los medios digitales.

PALABRAS CLAVE: propiedad intelectual, copyright, derechos de autor, Sociedad de la Información, economía del conocimiento, código de ingenios.

ABSTRACT: There is a narrow relationship between the Information Society and knowledge economy that needs to be reviewed. In this context, there are different ways to adapt the existing standards to copyright and intellectual property for digital media.

KEYWORDS: intellectual property, copyright, information society, economy of knowledge, Wit Code.

La sociedad actual presenta oportunidades y retos antes no existentes. De esta manera, somos parte de la Sociedad de la Información, en donde las tecnologías de información y comunicación (TICs) han cambiado no solo la forma de ver el mundo, sino que han ocupado todas las esferas de nuestras vidas, trastocando de manera radical la forma de interrelacionarnos, comunicarnos y el modo en el que comercializamos. La Internet y las TICs se han convertido en herramientas indispensables para realizar nuestro trabajo y para sentirnos miembros más activos de la comunidad. Asimismo, nuestra sociedad se enfrenta a otro paradigma: la economía del conocimiento. Una economía que está basada en activos intangibles, derechos de propiedad intelectual y, por ende, creaciones del intelecto humano. La transformación de los mercados globalizados, por medio de la innovación tecnológica y de los negocios, ha hecho que el valor de mercado de las empresas pase a fundamentarse en activos intangibles en lugar de tangibles. Las estadísticas muestran que en 1975 el valor de mercado de las empresas era de un 83% activo tangible y un 17% activo intangible; hoy en día, el valor de los intangibles ocupa el 84% del valor total de mercado (Ocean Tomo, LLC, 2015).

Esta realidad nos enfrenta a una sociedad y economía dinámicas que tienen que estar preparadas para afrontar los cambios generados en esta época. Así, se debe tener claro que el sistema de propiedad intelectual posee dos dimensiones. Por un lado, ha sido concebido como un mecanismo de recompensa e incentivo para los inventores y creadores por su trabajo intelectual, a fin de que estos continúen creando e innovando y, de esta forma, se promueva el progreso de la sociedad. Por otro lado, el sistema de propiedad intelectual tiene su base en la divulgación, permitiendo que la sociedad acceda a la información, de forma que se convierta en un estímulo para la creación, competencia y generación de nuevos bienes y servicios para la satisfacción de necesidades.

> Intellectual property, very broadly, means the legal rights which result from intellectual activity in the industrial, scientific, literary and artistic fields. Countries have laws to protect intellectual property for two main reasons. One is to give statutory expression to the moral and economic rights of creators in their creations and the rights of the public in access to those creations. The second is to promote, as a deliberate act of Government policy, creativity and the dissemination and application of its results and to encourage fair trading which would contribute to economic and social development. (Wipo, 2004, p.3)

Es así que los derechos de propiedad intelectual han sido reconocidos como parte importante del desarrollo de los seres humanos y de la sociedad, no solo por los instrumentos nacionales e internacionales sobre Propiedad Intelectual, sino que también se encuentran contenidos en el art. 27 de la Declaración Universal de Derechos Humanos.

Artículo 27

> Toda persona tiene derecho a tomar parte libremente en la vida cultural de la comunidad, a gozar de las artes y a participar en el progreso científico y en los beneficios que de él resulten.
>
> Toda persona tiene derecho a la protección de los intereses morales y materiales que le correspondan por razón de las producciones científicas, literarias o artísticas de que sea autora.

Ahora bien ¿cuál es la interrelación existente entre la Sociedad de la Información y la economía del conocimiento? Tanto la Sociedad de la Información como la economía del conocimiento presentan varios aspectos y dimensiones, por lo que para efectos de esta investigación nos centraremos en el impacto del Internet en los derechos de autor, por considerarlos los más vulnerables en medios digitales. Es importante recalcar que otros derechos de propiedad intelectual como las marcas, derechos conexos e incluso en algunas legislaciones los derechos de patentes (software y modelos de negocios) también son susceptibles a ser infringidos en Internet, no obstante, son los derechos de autor los que se podría decir generan mayor controversia por su repercusión directa en otros derechos, como el de libertad de expresión, acceso a la información, entre otros.

Internet tiene un impacto significativo como herramienta dinamizadora de la economía y de la transmisión de conocimiento. No obstante, al interactuar con los derechos de propiedad intelectual se puede determinar la existencia de una paradoja. De esta manera, si bien la Internet presenta aspectos positivos como facilitar la divulgación (cumpliendo así con uno de los objetivos de la propiedad intelectual) también hay efectos negativos, especialmente, en lo referente a la infracción y al ejercicio de los derechos de propiedad intelectual. Por tanto, es importante realizar un estudio sobre el impacto de la Internet en los derechos de autor con el fin de determinar hasta qué punto el Ecuador requiere una regulación especializada para el ciberespacio.

Por un lado las nuevas tecnologías han permitido la aparición de nuevas formas y soportes de creación, así como de nuevas formas de uso y utilización de obras intelectuales, es decir, siguiendo a J.A. GÓMEZ SEGADE, de nuevas formas de explotación que pueden constituir fuentes suplementarias de retribución de los autores, y facilitar la difusión de las obras intelectuales permitiendo un acceso global a las mismas sin restricciones territoriales, económicas o culturales. (…) Pero, por otro lado, estas mismas tecnologías dificultan la protección de los derechos de autor pues hacen muy difícil el control de la explotación de las obras, permitiendo no solo su reproducción rápida, a bajo coste, y sin merma de alguna calidad, sino también una fácil manipulación de dichas obras. Si a todo esto le sumamos el hecho de que las obras digitalizadas pueden ser puestas a disposición del público y comercializadas a nivel mundial a través de Internet, es evidente que se diluye el control del autor sobre su obra (Cremades, 2002, p.1405).

No se puede hablar de una definición única de los derechos de autor, por su naturaleza territorial; sin embargo, se puede establecer que el derecho de autor se ocupa de los derechos de los autores sobre su creación intelectual. El derecho de autor, por tanto, solo protege la forma de expresión de las ideas, no las ideas en sí mismas. De esta manera, al proteger la forma en la que se expresan las ideas, se está protegiendo la creatividad en la elección y disposición de palabras, notas musicales, colores, formas, entre otros. Así, derecho de autor otorga a sus titulares un derecho de exclusiva, por medio del que está facultado a evitar el uso no autorizado de la obra por parte de terceros (WIPO, 2004, p.40).

Por tanto, el objeto de protección de los derechos de autor incluye todas las producciones en el campo literario, científico y el dominio artístico, cualquiera que sea el modo o forma de expresión. Para que un trabajo pueda disfrutar de la protección dada por los derechos de autor, debe ser una creación original. Las ideas en el trabajo no necesitan ser nuevas, pero la forma, ya sea literaria o artística, en la que se expresan debe ser una creación original del autor (WIPO, s/f).

Los derechos de autor se encuentran regulados por el Convenio de Berna, mismo que se fundamenta en los principios de trato nacional, protección automática e independencia de la protección (Convenio de Berna, 1886). Asimismo, contiene las normas que determinan la protección mínima de obras literarias y artísticas que se concede al autor, además de que establece los derechos protegidos. De igual manera, el Convenio de Berna formula ciertas limitaciones y excepciones a los derechos patrimoniales de autor, de esta manera, se establecen ciertas condiciones y situaciones en las que las obras protegidas por el derecho de autor se convierten en obras de libre uso o acceso. También, se prevé la utilización de licencias no voluntarias u obligatorias de ser el caso. Esta normativa y estos principios han sido acogidos por los Acuerdos sobre los aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC), Decisión 351 y la normativa nacional.

El ADPIC es el tratado que regula los derechos de propiedad intelectual y establece un set de estándares mínimos orientados a reducir las distorsiones e impedimentos en el mercado internacional y promueve una protección adecuada de los derechos de propiedad intelectual entre los países miembros de la Organización Mundial de Comercio (OMC).Uno de los objetivos de los ADPIC es asegurar que las disposiciones relativas a la aplicación de los derechos de propiedad intelectual no constituyan en sí mismos obstáculos o barreras al comercio legítimo (Acuerdo sobre los aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio, 1994, Preámbulo).

El derecho de autor, al igual que el resto de derechos de propiedad intelectual, se fundamenta tanto en el interés público como en el derecho a la propiedad sobre las creaciones del intelecto humano. De esta manera, surgen las dos dimensiones de los derechos de autor: los derechos morales y los patrimoniales. Los primeros

se enfocan en el derecho del autor sobre la paternidad de su obra, mientras que los segundos se refieren a la explotación de la obra en sí. De esta manera, los derechos morales consisten en:

- Reivindicar la paternidad de su obra;
- Mantener la obra inédita o conservarla en el anonimato o exigir que se mencione su nombre o seudónimo cada vez que sea utilizada;
- Oponerse a toda deformación, mutilación, alteración o modificación de la obra que pueda perjudicar el honor o la reputación de su autor. Derecho de Integridad;
- Acceder al ejemplar único o raro de la obra que se encuentre en posesión de un tercero, a fin de ejercitar el derecho de divulgación o cualquier otro que le corresponda (Ley de propiedad Intelectual, 1998, Art. 18).

Por su parte, los derechos patrimoniales se enfocan en las formas de explotación de la obra, así:

- La reproducción de la obra por cualquier forma o procedimiento;
- La comunicación pública de la obra por cualquier medio que sirva para difundir las palabras, los signos, los sonidos o las imágenes;
- La distribución pública de ejemplares o copias de la obra mediante la venta, arrendamiento o alquiler;
- La importación; y,
- La traducción, adaptación, arreglo u otra transformación de la obra. (Ley de propiedad Intelectual, 1998, Art. 20).

En este sentido, se puede determinar que el Internet tiene un impacto en el derecho moral de deformación y principalmente en los derechos patrimoniales de reproducción, comunicación pública y distribución pública. El Internet pone al alcance una gran plataforma en la que el acceso a la información se facilita. Asimismo, la digitalización de obras ha hecho posible que los procesos de copia cada vez sean más rápidos y factibles.

Por otra parte, los derechos de autor no son derechos absolutos, por lo que existen limitaciones a estos derechos de exclusiva. De esta forma, ciertos actos normalmente restringidos por los derechos de autor, en circunstancias especificadas en la ley, pueden ser realizados sin la autorización del titular del derecho de autor. Estas excepciones se encuentran contenidas en el Art. 83 de la Ley de Propiedad Intelectual (LPI) en donde se establecen 11 casos mediante los que se puede hacer uso de una obra protegida por derechos de autor sin la autorización del titular. En algunas jurisdicciones como la americana se ha desarrollado la doctrina del *fair*

use o uso justo. Esta doctrina cubre un espectro más amplio que el abarcado por el Art. 83 de la LPI, ya que introduce parámetros de valoración para determinar si el uso del material protegido por derechos de autor es lícito o se está incurriendo en una infracción. La doctrina del *fair use* a pesar de haber sido desarrollada en la jurisprudencia, se encuentra codificada en 17 U.S.C. sección 107:

> Notwithstanding the provisions of sections 106 and 106A, the fair use of a copyrighted work, including such use by reproduction in copies or phono records or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include—
>
> (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;(2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work. The fact that a work is unpublished shall not itself bar a finding of fair use if such finding is made upon consideration of all the above factors (Merges et al., 2006, 507).

En virtud del esperado impacto del Internet en los derechos de autor, la normativa nacional e internacional entró a regular nuevos tipos de creaciones, así como formas de explotación. Es así como el ADPIC, además de acogerse a lo establecido en el Convenio de Berna, introduce una regulación en lo referente a programas de ordenador, bases de datos y nuevos medios de explotación como el alquiler.

De igual manera, en 1996 se adoptó el Tratado de la OMPI sobre Derechos de Autor (WCT por sus siglas en inglés), el cual entró en vigor en 2002 y del que el Ecuador es signatario. El WCT toma como fundamento lo establecido en el Convenio de Berna, pero lo hace extensivo a la protección de derechos de autor en medios digitales. El WTC establece como objetos de protección a los programas de ordenador y a las bases de datos. Asimismo, además de reconocer los derechos establecidos en el Convenio de Berna, el WTC establece los siguientes derechos: i) el derecho de distribución, ii) el derecho de alquiler y iii) un derecho más amplio de comunicación al público. Los mismos que han sido adaptados y creados para tener una consistencia con la realidad digital (Tratado de la OMPI sobre Derechos de Autor, 1996).

> El derecho de distribución es el derecho a autorizar la puesta a disposición del público del original y los ejemplares de la obra mediante venta u otra transferencia de propiedad.

> El derecho de alquiler es el derecho a autorizar el alquiler comercial al público del original y las copias de tres tipos de obras: i) los programas de ordenador (excepto cuando el programa propiamente dicho no sea el objeto esencial del alquiler); ii) las obras cinematográficas (pero únicamente cuando el alquiler comercial haya dado lugar a una copia generalizada de dicha obra que menoscabe considerablemente el derecho exclusivo de reproducción); y iii) las obras incorporadas en fonogramas, tal como lo establezca la legislación nacional de las Partes Contratantes.
>
> El derecho de comunicación al público es el derecho a autorizar cualquier comunicación al público por medios alámbricos o inalámbricos, comprendida "la puesta a disposición del público de sus obras, de tal forma que los miembros del público puedan acceder a estas obras desde el lugar y en el momento que cada uno de ellos elija". La expresión citada abarca, en particular, la comunicación interactiva y previa solicitud por Internet. (WIPO, Reseña del Tratado de la OMPI sobre Derecho de Autor (WCT) (1996)).

Aun cuando el derecho de reproducción es uno de los que se encuentra más vulnerado en medios digitales, el WTC decidió que, para fines del tratado, el concepto sobre derechos de reproducción establecido en el Art. 9 del Convenio de Berna aplica perfectamente al medio digital, en particular al uso de obras digitalizadas (Tratado de la OMPI sobre Derechos de Autor, 1996). No obstante, el derecho de reproducción fue uno de los más controversiales en la discusión del WTC, por cuanto países como la U.E., EE.UU y otros respaldaban la tesis de la OMPI en la que se "proponía una obligación de autorización previa del autor para la reproducción de manera directa o indirecta, permanente o provisional, por cualquier procedimiento y bajo cualquier forma" (Solines, s/f, p.4), postura que puede llegar a infringir los derechos de libertad de expresión y el acceso a la información.

De igual manera, el WCT establece ciertas limitaciones y excepciones a los derechos de autor, para lo que sigue lo establecido en el Convenio de Berna en lo referente a la regla o test de los tres pasos. La regla de los tres pasos se resume básicamente en que se permite, en ciertas circunstancias, la reproducción de la obra sin previa autorización del autor, siempre que esta reproducción no atente a la explotación normal de la obra ni cause un perjuicio injustificado a los derechos del autor. "En las Declaraciones concertadas que acompañan al WCT se estipula que esas limitaciones y excepciones, establecidas en la legislación nacional de conformidad con el Convenio de Berna, podrán hacerse extensivas al entorno digital" (WIPO, Reseña del Tratado de la OMPI sobre Derecho de Autor (WCT) (1996)). Se deja claro que se pueden mantener las existentes o crear más, siempre que se cumpla la regla de los tres pasos. Con respecto a la interpretación de este test o regla, el instituto Max Planck ha emitido una declaración en la que establece que la regla de los tres pasos debe ser ponderada en función de otros factores. De esta manera, señala:

> Por el contrario, los tres pasos de la prueba en su conjunto deben considerarse como una "evaluación exhaustiva de conjunto" que tome en cuenta las amenazas excesivas que los niveles de protección a los derechos de autor representan para "los derechos humanos y las libertades fundamentales de las personas", " los intereses en competencia", y "los otros intereses públicos, en particular en el progreso científico y el desarrollo cultural, social o económico", además de los importantes intereses de los titulares de derechos de autor en la búsqueda de una compensación justa (Electronic Frontier Foundation, s/f, p.2).

Por otro lado, en el caso ecuatoriano, la Ley de Propiedad Intelectual ha incorporado ciertas definiciones y normas orientadas a la regulación de derechos de autor en entornos digitales, de esta manera, al definir y regular el derecho de reproducción se incluye, dentro de este concepto, al almacenamiento digital temporal o definitivo. De igual manera, establece que la "reproducción consiste en la fijación o réplica de la obra por cualquier medio o por cualquier procedimiento, conocido o por conocerse, incluyendo su almacenamiento digital, temporal o definitivo (…)" (Ley de Propiedad Intelectual, 1998, Art. 21), de lo que se desprende que la norma no solo trata de regular el derecho de reproducción en medios digitales, sino que contempla incluso cualquier nueva tecnología a futuro. No obstante, la norma es insuficiente, ya que no establece de forma clara la aplicación de las limitaciones o excepciones a los derechos de reproducción en línea, de forma que se tendría que aplicar el Art. 83 en los entornos digitales, lo que es insuficiente, por cuanto las excepciones son de carácter taxativo y no proveen ningún criterio de evaluación que permita extender de manera más factible estas excepciones a medios digitales, como podría ser la doctrina del *fair use* que no ha sido acogida por nuestro sistema.

Asimismo, la Ley de Propiedad Intelectual, al tratar el tema de la protección y observancia de los derechos de propiedad intelectual, regula en el artículo 292 la violación a través de redes de comunicación digital y dispone:

> Art. 292. Si la violación de los derechos se realiza a través de redes de comunicación digital, tendrá responsabilidad solidaria el operador o cualquier otra persona natural o jurídica que tenga el control de un sistema informático interconectado a dicha red, a través del cual se permita, induzca o facilite la comunicación, reproducción, transmisión o cualquier otro acto violatorio de los derechos previstos en ésta Ley, siempre que tenga conocimiento o haya sido advertido de la posible infracción, o no haya podido ignorarla sin negligencia grave de su parte.
>
> Se entenderá que ha sido advertido de la posibilidad de la infracción cuando se le ha dado noticia debidamente fundamentada sobre ella (Ley de Propiedad Intelectual, 1998, Art. 292).

Este artículo, si bien trata de proteger el cumplimiento de los derechos de propiedad intelectual, es desproporcional, pues el momento en que se establece la responsabilidad solidaria del operador o cualquier persona natural o jurídica que tenga el control del sistema informático, se crea una censura previa que puede dar lugar a la afectación de otros derechos. De esta manera, si bien la norma establece que la violación se da cuando el operador ha sido advertido de la posible infracción por medio de una noticia "debidamente fundamentada", esta norma inhibe a los operadores de sus actividades, dando lugar a casos de censuras y baja del contenido de forma inapropiada e incluso abusiva. (Sanja, et al. 2013).

De igual manera, en el Ecuador se ha utilizado a la protección de derechos de autor para prohibir el uso de contenido e imágenes relacionadas con el Presidente de la República y con temas de gobierno en entornos físicos y digitales. Entonces, las autoridades han generado una censura improcedente que se va en contra de la misma ley de propiedad intelectual, la que establece que estos usos son considerados como actos lícitos que no requieren autorización del titular y, por ende, se encuentran contemplados en las excepciones del art. 83. Del mismo modo, este tipo de arbitrariedades van en contra del verdadero titular de los derechos de autor, quien es el fotógrafo que ha tomado la foto o ha hecho el video del Presidente o del acto en mención.

> The Ecuadorian government has periodically sought to block critical content on grounds of copyright infringement. A controversial 2012 documentary about President Correa was subject to such treatment when clips of the films were posted on YouTube and Vimeo. The videos were removed after Spanish anti-piracy firm Ares Rights filed a copyright infringement lawsuit on behalf of Ecuador's state-run TV channel, claiming that the documentary included unauthorized images of the president. Distribution of the documentary has been riddled with problems both within Ecuador and abroad ever since (Sanja, et. al, 2013, p.236).

Lo anteriormente expuesto, explica el marco normativo de los derechos de autor en Internet. Si bien no existe una normativa exhaustiva en esta área a nivel nacional, la normativa existente ha causado más complicaciones que ventajas, como es el caso del art. 292 de la LPI y el uso abusivo e inadecuado de la protección de derechos de autor por parte de las autoridades actuales, lo que ha traído como principales efectos la censura de contenidos, violación a la normativa de derechos de autor y una limitación al derecho de libertad de expresión constitucionalmente protegido. Ahora bien, es necesario identificar si se requiere de una normativa expresa para regular los derechos de autor en Internet o si, por el contrario, la normativa existente es suficiente. Al respecto, se considera necesario realizar un análisis sobre el caso americano en el que existe una normativa específica para regular el tema de derechos de autor en Internet, esto con el fin de determinar su eficacia.

Estados Unidos ha sido uno de los pioneros en lo que a la regulación de derechos de autor en el Internet se refiere. Por esta razón y con el fin de implementar el Tratado de la OMPI sobre derechos de Autor (WTC) y el Tratado sobre Interpretación o Ejecución de fonogramas, se creó la Digital Millennium Copyright Act (DMCA), la misma que aborda temas de relevancia y que están relacionados con los derechos de autor en la era digital.

La DMCA se divide en cinco títulos. El primero está relacionado con la implementación de los tratados de la WIPO antes mencionados. El segundo trata sobre las limitaciones y responsabilidades ante la violación de derechos de autor en línea, así la DMCA crea limitaciones para la responsabilidad de los proveedores de servicios en línea por infracción de copyright al participar en ciertos tipos de actividades. El tercero se refiere al seguro en el mantenimiento de computadoras, de esta manera, la norma crea una exención para hacer una copia de un programa de ordenador, mediante la activación de un ordenador para fines de mantenimiento o reparación. El cuarto contiene seis artículos en los que se regulan las funciones de la Oficina de Derechos de Autor, la educación a distancia, las excepciones previstas en la Ley de derechos de autor para las bibliotecas y para realizar grabaciones efímeras, "difusión por Internet" de las grabaciones sonoras en Internet y la aplicabilidad del convenio colectivo de obligaciones en el caso de las cesiones de derechos de imágenes en movimiento. Y el quinto que crea una nueva forma de protección para el diseño de cascos de los buques (U.S. Copyright Office Summary, 1998).

El objetivo de la DMCA, al implementar los tratados de la OMPI, estaba dirigido a precautelar los derechos de los autores en Internet de una forma efectiva, eliminando así la piratería y parando la *black box* en la industria de la música. No obstante, el resultado de la implementación de la DMCA está lejos de ser lo planteado, pues se ha convertido en un instrumento que en lugar de parar a los piratas cibernéticos, ha distorsionado la doctrina del *fair use*, impidiendo que científicos, investigadores, estudiantes, consumidores y usuarios, en general, tengan acceso a trabajos protegidos que bajo la mencionada doctrina hubiesen sido permitidos (Electronic Frontier Foundation, 2010).

De esta manera, las provisiones *anti-circumvention*, contenidas en la DMCA, en lugar de ser un mecanismo para parar las violaciones a derechos de autor, se han convertido en una medida para reprimir actividades legítimas. Consecuentemente, se han vuelto una amenaza para el ejercicio de varios derechos. Así, la DCMA ha transgredido los derechos de libre expresión e investigación científica, ha puesto en peligro la aplicación y supervivencia de la doctrina del *fair use* y se ha constituido en un mecanismo que atenta contra la competencia e innovación y que puede ser usado como prohibición de uso general en el acceso a la red informática (Electronic Frontier Foundation, 2010).

> At its core, the DMCA flatly prohibits the circumvention of "technological protection measures "in order to gain access to copyrighted works, but

> provides no safety valve for any traditionally protected uses. While hailed as a victory by the software and entertainment industries, the academic and scientific communities have been far less enthusiastic. The DMCA's goal of combating piracy is a noble one, but lurking is the danger that it comes at the expense of public access to protected works and future innovation. Despite America's long history of "fair use" protections in copyright law, commentators have warned that consumers now find themselves unable to do many of the same things with copyrighted works that they previously could-anyone who might sell them the technology to access a protected work and enable fair use would find themselves in violation of the DMCA. Worse, early litigation dramatically expanded the definition of what constitutes a "technological protection measure" deserving of the law's respect. As the definition broadened, scholars feared that even modest innovations-ones that would never qualify for a patent under existing law--could wind up receiving perpetual patent-like protection through the backdoor of the DMCA. Despite the experts' dire predictions, however, subsequent common law interpretation of the DMCA has reined in many of its potential dangers. The judiciary's focus has rightly shifted to the need to balance innovators' interests with the equally important goals of public access and enhancing overall social welfare (Calandrillo & Davison, 2008, pp.349-350).

Por tanto, si bien se deben tener claras las complicaciones que existen para el efectivo ejercicio de los derechos de autor en el Internet, no se puede desconocer que regulaciones específicas para este medio pueden dar lugar a un ejercicio abusivo de los derechos de autor, desconociendo las limitaciones y excepciones establecidas en la normativa nacional e internacional y dando lugar a una vulneración de otros derechos. De igual manera, una excesiva regularización del Internet mataría su esencia libre y dinámica, acabando con los procesos de innovación que ofrece la red.

Consecuentemente, si se parte de que los derechos de autor ya se encuentran regulados de forma general, y que además existen tratados específicos sobre la regulación de derechos de autor en medios digitales y, además, tomando en cuenta la experiencia existente, se considera que no debe haber una regulación específica de los derechos de autor en Internet, pues esto es irse en contra de la naturaleza de la red, en contra de uno de los fines de la propiedad intelectual como es la divulgación y la innovación. De ahí que se considere que sería importante para el Ecuador adoptar parámetros de evaluación para el uso legítimo de derechos de autor sin autorización del titular, lo que nos acercaría a la doctrina del *fair use.* Las limitaciones a los derechos de autor existentes en la ley de propiedad intelectual, al ser puntuales, dejan de ser aplicables de forma eficaz en medios digitales, de ahí que la adopción de criterios de ponderación, como los recogidos en la sección 17 U.S.C. sección 107 y que son parte de la doctrina del *fair use*, podrían dar un espectro más

certero que permita una protección de los derechos de autor y, a la vez, permitiría que usuarios accedan libre y legítimamente a información protegida bajo la premisa de las limitaciones de los derechos de autor.

Si bien es cierto ha habido casos de violaciones a los derechos de autor en Internet, como en caso de Napster[1], en el que la Corte, luego de la aplicación de la doctrina del *fair use*, determinó la violación de los derechos de autor; también se tiene que dar crédito a estos inicios, ya que, por medio de los mismos, surgieron nuevas formas de innovación en los negocios, como Spotify y iTunes, que son plataformas que, si bien sirven para acceder a música, permiten también recuperar las regalías y entregárselas a los titulares de derechos de autor. De esta manera, Spotify, con su innovador mecanismo para la reproducción de música en línea, ha logrado convertirse en un sistema para que los titulares de derechos de autor en el campo de la música puedan obtener sus regalías. Es importante señalar que el sistema aún presenta problemas e incluso se ha visto involucrado en presuntos casos de violación de derechos de autor (Fortune, 2015). No obstante, a pesar de sus falencias, representa una alternativa para usuarios y titulares, convirtiéndose en un sistema perfectible que potencia el respeto de los derechos de autor a la vez que contribuye a la diseminación de las composiciones musicales.

Actualmente, en el Ecuador se está discutiendo el proyecto del Código Orgánico de Economía Social del Conocimiento e Innovación (Código Ingenios), su objeto es “generar un marco legal en el que se estructure la economía social de los conocimientos, la creatividad y la innovación”(Código Ingenios, Art.1). El Código Ingenios concibe al conocimiento como un bien de interés público y tiene como base la democratización del mismo. Establece así, dentro de sus principios, que “El conocimiento constituye un bien de interés público, su acceso será libre y no tendrá más restricciones que las establecidas en este Código, la Constitución, los tratados e instrumentos internacionales y la Ley; y, su distribución se realizará de manera justa, equitativa y democrática” (Código Ingenios, Art.4). Con estas premisas, el Código Ingenios, a pesar de manifestar su consistencia con el ADPIC, contiene disposiciones no solo contrarias, sino que atentan contra la doble dimensión de la propiedad intelectual.

En el área de derechos de autor, si bien el Código mantiene elementos fundamentales de la Ley de Propiedad Intelectual, también introduce cambios sustanciales y establece un régimen sensible e incluso confiscatorio. No obstante, no entraremos a analizar la compleja problemática que introduce el Código Ingenios en el área de derechos de autor y procederemos a centrarnos únicamente en los cambios que introduce a nivel de derechos de autor en Internet.

El Código Ingenios, en el parágrafo tercero, de la Sección IV: Contenido del Derecho de Autor, introduce disposiciones orientadas a implantar medidas tecnoló-

1 *Véase* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

gicas para la gestión y protección de derechos. De esta manera, establece de forma taxativa la posibilidad de los titulares de derechos de autor y conexos para establecer "medidas tecnológicas efectivas, como sistemas de cifrado u otros, respecto de sus obras y prestaciones protegidas por derechos de autor y derechos conexos, que restrinjan actos no autorizados por los titulares o establecidos en la legislación" (Código Ingenios, Art.21). Esta norma no es necesaria dentro de nuestro ordenamiento jurídico, porque la adopción de medidas tecnológicas para la protección y obras protegidas está a disponibilidad y opción de los titulares de derechos, el hecho de establecer de manera expresa dentro de la normativa de propiedad intelectual, podría dar lugar a una proliferación de estos mecanismos e incluso a la generación de un estándar para la gestión de obras protegidas e información en general, entorpeciendo el acceso a la información y a contenidos que se encuentran en el dominio público e incluso impidiendo el ejercicio de las limitaciones y excepciones para contenidos protegidos por derechos de autor establecidos en la normativa nacional, comunitaria e internacional. Asimismo, la incorporación de mecanismos o medidas tecnológicas para la gestión de derechos ha demostrado no ser efectiva y generar algunos inconvenientes no solo a nivel legal, sino a nivel de industria y mercado en general, así:

> While DRM uses various technologies to secure digital content, it is not only a technological phenomenon. From an organizational perspective, DRM interoperability and standardization remain open problems to a large extent. From a business perspective, it is intriguing to examine the new business models which DRM systems could enable. From an economic perspective, DRM could challenge -jointly with other technologies associated with the Internet - some aspects of the standard economic theory taken for granted hitherto. From a sociological perspective, DRM could have an influence on the distribution of information and therefore power in a society. From a legal perspective, DRM creates a whole assemblage of problems ranging from copyright, contract, privacy, patent and antitrust problems to freedom of speech issues (Stefan Bechtold, 2004, pp. 324-325).

Teniendo como objetivo minimizar el impacto del Art.121, el Código Ingenios incorpora en su Art. 123 la obligatoriedad a los titulares de los derechos que han incorporado medidas tecnológicas de gestión de derechos de autor y conexos para que proporcionen, de forma oportuna, los medios para dejar sin efecto o neutralizar las medidas tecnológicas adoptadas para usuarios que quieran hacer uso de información en el dominio público o que estén dentro de las limitaciones y excepciones de los derechos de autor (Código ingenios, Art.123). Este artículo muestra, de forma evidente, lo absurdo del contenido del Art.121, pues la misma norma, de manera implícita, reconoce las restricciones, innecesarias, que se generan a los usos legítimos de contenidos e información. De esta manera, intenta, fallidamente, eliminar las restricciones creadas, a través del establecimiento de la obligación a los titulares de derechos, para que proporcionen las medidas para el acceso a la

información, sin considerar que una vez implementadas las medidas, el proceso de filtrado para autorizar el acceso sería ineficiente y discrecional, vulnerando así los derechos de los usuarios de contenidos e información.

> In the real world, "bare" DRM doesn't really do much. Before governments enacted laws making compromising DRM illegal (even if no copyright infringement took place), DRM didn't survive contact with the market for long. That's because technologically, DRM doesn't make any sense. For DRM to work, you have to send a scrambled message (say, a movie) to your customer, then give your customer a program to unscramble it. Anyone who wants to can become your customer simply by downloading your player or buying your device – "anyone" in this case includes the most skilled technical people in the world. From there, your adversary's job is to figure out where in the player you've hidden the key that is used to unscramble the message (the movie, the ebook, song, etc). Once she does that, she can make her own player that unscrambles your files. And unless it's illegal to do this, she can sell her app or device, which will be better than yours, because it will do a bunch of things you don't want it to do: allow your customers to use the media they buy on whatever devices they own, allow them to share the media with friends, to play it in other countries, to sell it on as a used good, and so on. The only reason to use DRM is because your customers want to do something and you don't want them to do it. If someone else can offer your customers a player that does the stuff you hate and they love, they'll buy it. So your DRM vanishes (The Guardian, 2014).

Dentro del mismo parágrafo, el Código Ingenios en el Art. 122 incluye una paráfrasis del Art. 26 de la Ley de Propiedad Intelectual, a la que incorpora una peligrosa prohibición. De esta manera, establece que: "Se prohíbe realizar cualquier acto que tenga como finalidad inducir, permitir, facilitar u ocultar la infracción de cualquiera de los derechos previstos en el presente título." Esta disposición es sensible, por cuanto, sin llegar a la criminalización de actos orientados a la eliminación de medidas tecnológicas de gestión, como la DMCA, la prohibición puede generar un efecto inhibidor, en el que usuarios que pretendan un uso legítimo de contenidos protegidos por derecho de autor o de dominio público, que estén protegidos por medidas tecnológicas, opten por no acceder a la información para no incurrir en la prohibición. Estos, sin duda, como ha sido mencionado anteriormente, son mecanismos que van en contra de la competencia y la innovación, sin mencionar la restricción de derechos.

Además, el Código Ingenios, en el parágrafo segundo, de la Sección VII: De las limitaciones y excepciones a los derechos patrimoniales, en su Art. 197, incorpora al ordenamiento jurídico la doctrina del uso justo. De esta manera, se adoptan los parámetros desarrollados por la jurisprudencia norteamericana, contemplados en el 17 U.S.C. sección 107. De esta manera:

> Artículo 197.- Uso justo de una obra.- El uso justo de una obra no constituirá una violación de los derechos patrimoniales sobre la misma. Para determinar si el uso de la obra se adecua a lo dispuesto en este artículo se tendrá en cuenta lo establecido en este Código y en los tratados internacionales de los que Ecuador es parte, así como entre otros, los siguientes factores: Si el uso de la obra es para fines educativos y no lucrativos; Los objetivos y la naturaleza del uso; La naturaleza de la obra; La cantidad y la importancia de la parte usada en relación con la obra en su conjunto; y, El efecto del uso en el valor de mercado actual y potencial de la obra (Código Ingenios, Art. 197).

Al respecto, estamos de acuerdo con esta limitación, por cuanto, al establecer parámetros más flexibles de evaluación sobre el uso de obras protegidas por derechos de autor, se garantiza el acceso para usos legítimos, cumpliendo así, una de las dimensiones de la propiedad intelectual, como son: la difusión del conocimiento y la promoción de la actividad creativa. Asimismo, consideramos que la doctrina del uso justo permite una aplicación en medios digitales y garantiza, por un lado, los derechos de autor y, por otro, los derechos de usuarios en Internet. No obstante, el Código Ingenios incluye una lista, aparentemente ejemplificativa, en la que no se requiere la autorización de los titulares de derechos para el uso de material protegido en 26 escenarios. La incorporación de estos usos genera una contradicción con respecto a la doctrina del uso justo, en razón de que esta plantea que se debe aplicar el test con todos sus criterios en cada escenario, de forma que no podemos encasillar al uso justo por categorías o situaciones generalizadas, ya que se debe analizar el contexto de manera individual; así, mal podemos decir que todo uso para fines de enseñanza es justo, en razón de que se debe aplicar el test a la circunstancia concreta. Por tanto, el Art. 198 del Código Ingenios debería ser eliminado, por constituir una amenaza al ejercicio efectivo de los derechos de autor.

> To determine whether a use is or is not a fair use, always keep in mind that you need to apply all four factors. For example, do not jump to a conclusion based simply on whether your use is educational or commercial. You still need to evaluate, apply, and weigh in the balance the nature of the copyrighted work, the amount or substantiality of the portion used, and the potential impact of the use on the market or value of the work. This flexible approach to fair use is critical in order for the law to adapt to changing technologies and to meet innovative needs of higher education. Not all factors need to weigh either for or against fair use, but overall the factors will usually learn one direction or the other (Columbia University Libraries, s/f).

Por tanto, consideramos que, dado el dinamismo del Internet y la doble dimensión de los derechos de autor, se debería optar por la generación de modelos de negocio e intercambio de contenidos que coadyuven tanto a la protección de derechos de autor como al acceso a la información. De esta manera, podemos

afirmar que la normativa existente es suficiente y que tan solo debe adaptarse, de manera creativa, respetuosa y legítima a los medios digitales. Así, no es necesaria una regulación específica sobre los derechos de autor en Internet, pues como hemos demostrado anteriormente, esta normativa es poco eficiente para el cumplimiento de los derechos de autor y, por el contrario, produce efectos adversos en la interacción de los usuarios y en el acceso a contenidos, vulnerando derechos de mayor jerarquía. De ahí que consideremos que las normas establecidas en el Código Ingenios no pueden ser aprobadas tal como se encuentran en el Proyecto, pues esto coadyuvaría a la vulneración, no solo de derechos de autor, sino incluso de derechos fundamentales.

Bibliografía:

Acuerdo sobre los aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio. (1994).

Bechtold, Stefan (2004). "Digital Digital Rights Management in the United States and Europe". *The American Journal of Comparative Law,* Vol. 52, No. 2, pp. 323-382

Calandrillo & Davison (2008). "The dangers of the Digital Millennium Copyright Act: much ado about nothing?". *William and Mary Law Review*, vol 50, issue 2.

Código Orgánico de Economía Social del Conocimiento e Innovación (Proyecto).

Columbia University Libraries- Copyright Advisory Office. "Fair Use".Columbia University < *https://copyright.columbia.edu/basics/fair-use.html>,* [19/07/2016].

Convenio de Berna. (1886).

Cremades, J. (2002). *Régimen Jurídico de Internet.* Madrid: La Ley.

Decisión 351 CAN. (1993).

Declaración Universal de Derechos Humanos. (1948).

Digital Millennium Copyright Act. (1998).

Electronic Frontier Foundation. "La Prueba de los Tres Pasos". *Eff.org* <https://www.eff.org/files/filenode/tpp_3pasos.pdf>, [10/06/2016].

Electronic Frontier Foundation. "Unintended Consequences: Twelve Years under the DMCA". *Eff.org < https://www.eff.org/wp/unintended-consequences-under-dmca>,* [26/06/2016].

Fortune, "Spotify hit with $150 million copyright Infringement Lawsuit", <http://fortune.com/2015/12/29/spotify-150-million-lawsuit/>, [27/06/2016].

Ley de Propiedad Intelectual. (1998).

Mergers, Menell & Lemley (2006). *Intellectual Property in the New Technological Age*. New York: Aspen Publishers.

Ocean Tomo, LLC. "Ocean Tomo Releases 2015 Annual Study of Intangible Asset Market Value". *Insights Blog* < http://www.oceantomo.com/blog/2015/03-05-ocean-tomo-2015-intangible-asset-market-value/>, [07/06/2016].

Sanja et. al. "Freedom on the net 2013 a Global Assessment of Internet and Digital Media". *Freedomhouse <https://freedomhouse.org/sites/default/files/resources/FOTN%202013_Full%20Report_0.pdf>*, [15/06/2016].

Solines, Pablo. "La responsabilidad civil extracontractual de los prestadores de servicios de la sociedad de la información —intermediarios—, por infracciones cometidas a los derechos de autor y derechos conexos. Caso de Ecuador en comparación con la legislación europea" <http://www.solines.ec/docs/downloads/Responsabilidad%20de%20los%20PSSI%20por%20infracciones%20a%20la%20PI%20Ecuador.pdf>, [22/06/2016].

The Guardian. "What happens with digital rights management in the real world?" <https://www.theguardian.com/technology/blog/2014/feb/05/digital-rights-management>, [19/07/2016].

Tratado de la OMPI sobre Derechos de Autor. (1996).

U.S. Copyright Office Summary. "The Digital Millennium Copyright Act of 1998" <http://www.copyright.gov/legislation/dmca.pdf>, [20/06/2016].

WIPO (2004). *Wipo Intellectual Property Handbook*. Geneva: WIPO Publication.

WIPO. "Principios Básicos del Derecho de Autor y los Derechos Conexos". <http://www.wipo.int/edocs/pubdocs/es/intproperty/909/wipo_pub_909.pdf>, [23/06/2016].

WIPO. "Reseña del Tratado de la OMPI sobre Derecho de Autor (WCT) (1996)". *WIPO <http://www.wipo.int/treaties/es/ip/wct/summary_wct.html>,* [07/06/2016].

La insuficiencia de la regulación: lecciones para el internet a partir de la desregulación de la blasfemia

Pier Pigozzi
Universidad San Francisco de Quito

RESUMEN: La historia sobre la tensión perenne entre la libertad de expresión y la libertad de religión tiene mucho que enseñarnos al momento de discutir sobre la regulación de cualquier libertad para favorecer el goce paralelo de otros derechos. En este artículo, al punto de fricción entre la libertad de expresión y la libertad religiosa, lo llamaremos blasfemia y la discusión de su regulación se presenta como una serie de lecciones que deberíamos tener en cuenta en Ecuador, al momento de abordar la regulación del uso y acceso al internet.

PALABRAS CLAVE: Libertad de expresión, libertad de religión, internet, difamación, blasfemia, interdependencia de los derechos humanos.

ABSTRACT: The persistent tension between freedom of expression and freedom of religion has much to teach when addressing the regulation of any freedom in order to favor the concurrent enjoyment of other rights. For this article, the conflict between freedom of expression and religious freedom will be referred as blasphemy, and the lessons learned in the debate about its (de)regulation will be presented as considerations to bear in mind when addressing internet regulations in Ecuador.

KEYWORDS: Freedom of expression, freedom of religion, internet, defamation, blasphemy, human rights, interdependence.

1. Introducción

El internet no se caracteriza por ser un espacio sin regulaciones; por el contrario, las posibilidades de dessarrollo y uso del internet siempre han estado condicionadas tanto por las reglas de sus propios códigos informáticos de programación, como por las normas de propiedad intelectual (Lessig 1999, 2001, 2006). Además, la regulación del Internet no es solamente del tipo horizontal (del tipo que se crea a través de una suerte de consenso por la "comunidad global" de pares), sino que continúa siendo primordialmente vertical (del tipo que es promulgada por los estados) (Shultz, 2008, p. 799-801).

Estas constataciones de Lessig y Shultz nos demuestran que el entusiasmo inicial de vivir en una comunidad global, en una nube desregulada donde el flujo de información parecía ser irrestricto, pronto encontró las mismas necesidades prácticas que siempre encontrará cualquier espacio para la sociabilización humana. Los seres humanos vivimos según valores y preferencias que cultivamos dentro de las comunidades que naturalmente conformamos y que son indispensables para nuestra supervivencia material e inmaterial. El respaldo que requerimos para promover los planes de vida que escogemos, lo encontramos dentro de estas comunidades, y ellas son las que nos ayudan a desarrollar y defender las prácticas y los valores indispensables para el florecimiento de todos conforme nuestros propios planes de vida. Las necesidades de regulación, e incluso la de prohibición, son connaturales a la necesidad de coordinación que surge en toda comunidad que busca la previsibilidad en las relaciones de sus miembros para potenciar la realización de todos y también de cada uno ellos (es decir, para promover el bien común) (Finnis, 2011, pp. 100-291).

Estas afirmaciones de razonabilidad práctica sobre la necesidad connatural a toda asociación humana de coordinación y, por lo tanto, de las nociones de Derecho, obligación y autoridad, han sido ratificadas en la vivencia práctica de las últimas décadas en el internet. Shultz nos explica cómo las comunidades internautas pasaron del entusiasmo inicial de haber hallado un espacio sin regulaciones para buscar y distribuir información, a la preocupación francesa de que el internet se pudiera constituir en un espacio para la difusión de las antisemitas y radicalmente prohibidas negaciones sobre el holocausto, o la agitación estadounidense de que se pudieran propagar casinos en línea a pesar de sus restricciones legales estrictas (p. 804). En otras palabras, la necesidad de protección de los valores propios de cada comunidad no tardó en demandar la protección que se expresa a través de normas verticales aprobadas por autoridades estatales competentes. La reflexión a la que apunta este artículo es que esta necesidad natural de contar con un Derecho que

sirva como un instrumento de coordinación para la vida en comunidad no tiene que expresarse en forma de prohibición y que la regulación no debe entenderse como un sinónimo de restricción, sino que bien orientada puede ser un instrumento para promover la realización personal.

Es innegable que la aparición de nuevos espacios para actividades humanas siempre invitará a la aparición de normas y principios jurídicos que las regulen.[1] Hay, en efecto, asuntos de seguridad global que siempre requerirán de regulación jurídica e incluso de prohibiciones y sanciones de las más severas que un ordenamiento jurídico pueda aplicar. Sin embargo, entre el extremo de asuntos como la prohibición de tortura, la prohibición de pornografía infantil o la sanción del tráfico de personas, armas y drogas, y el otro extremo de las transacciones y actividades más inofensivas, hay un sinnúmero de otros usos del internet que no necesitan de prohibiciones, ni sanciones, pero sí pueden requerir de una regulación adecuada que facilite, y no impida, su uso y desarrollo. En las secciones siguientes discutiremos cuáles son las mejores alternativas a través del ejemplo de la regulación de la libertad de expresión con el fin de prevenir la ofensa a los sentimientos de religiosidad de terceros.

2. Una historia fallida de regulaciones

La tensión perenne entre la libertad de expresión y la libertad de religión tiene mucho que enseñarnos al momento de discutir sobre la regulación de cualquier libertad para favorecer la realización de la persona y el bien común. En este artículo, al punto de fricción entre la libertad de expresión y la libertad religiosa lo llamaremos blasfemia y la discusión de su regulación se presentará como una serie de lecciones que deberíamos tener en cuenta en Ecuador, al momento de abordar la regulación del uso y acceso al internet.

La colisión entre la libertad de expresar y el derecho a no ser ofendido en las convicciones más íntimas y trascendentales de la condición humana ha pasado por varios estados, los mismos que han tratado de solucionar jurídicamente las constantes amenazas que cada una de estas libertades ha puesto sobre la otra. La censura arbitraria y otras formas de violación a la libertad de expresión son una realidad palpable en el Ecuador contemporáneo, pero resulta casi impensable que la denigración de las creencias religiosas pueda ser un móvil para provocar violaciones atroces a los derechos humanos. Como veremos en los siguientes párrafos, la historia reciente nos demuestra todo lo contrario.

Además del lugar común del holocausto judío, el genocidio de *bosniaks* (musulmanes bosnios) y de serbios ortodoxos en Kosovo constituyen dos de las más

1 El internet no es el único ejemplo, la misma dinámica se podría observar cuando la humanidad encontró y empezó a hacer uso de los denominados espacios comunes como la Antártida, las órbitas geoestacionarias, el mar abierto, etc.

recientes atrocidades cometidas contra grupos religiosos al otro lado del Atlántico (Meierhenrich, 2014), donde existe una larguísima historia de persecución y agresión que fue justificada o exacerbada por motivos religiosos y que, actualmente, abre un nuevo capítulo contra el islam, que es la religión practicada por la mayoría de personas que han llegado a Europa en el éxodo masivo de refugiados sirios. Frecuentemente erramos de nuestro lado del Atlántico pensando que la protección de las libertades religiosas es una figura obsoleta en el presente del derecho internacional de los derechos humanos (Carozza, 2012) y olvidamos que en las Américas también tenemos episodios de espantosas ejecuciones y de otras violaciones a los derechos humanos que encontraron su origen, justificación o agravante en la religión del enemigo. Solo por citar un ejemplo: chamanes, sacerdotes y pastores, así como sus comunidades de creyentes, todos han sido blancos predilectos de proyectos políticos autoritarios de cualquier tendencia, a causa de su lenguaje de trascendencia en cuanto al valor de la vida humana y de su orientación hacia la libertad contra la opresión presentada con un lenguaje de cohesión comunitaria (Mayer, 2013; Research Directorate, Immigration and Refugee Board of Canada, 2006; Keogh, 1981).

La principal amenaza a la seguridad mundial proviene justamente del terrorismo que utiliza sentimientos de religiosidad para articular enemistades e incitar atrocidades como la difusión mediante el internet de episodios de decapitación, atentados contra diferentes escuelas antagónicas dentro del islam y el genocidio de cristianos en el Medio Oriente y en África, esto sin hacer mención a un sinnúmero de fenómenos de persecución religiosa de mediana y baja intensidad (Traslosheros, 2012), cuya acumulación es uno de los detonantes para actos de violencia que podrían menguarse si tomásemos con mayor seriedad la necesidad de proteger la libertad de religión en el discurso público.

Justamente en respuesta a esa necesidad, la experiencia europea frente a siglos de persecución religiosa y de guerras libradas en nombre de la religión[2] llevó a consagrar, de manera global, a la libertad religiosa como uno de los pilares del respeto a la dignidad humana. "La libertad de adorar a Dios a la manera propia de cada quien" (Roosevelt, 1941) fue una de las cuatro ideas básicas que, junto a la libertad de palabra, se invocaron a fin de congregar al mundo de posguerra para sentar todo el andamiaje actual del derecho internacional de los derechos humanos.[3] Fue así que el respeto y la promoción de la libertad religiosa y la libertad de

2 William Cavanaugh ha presentado una extensa investigación histórica cuyos resultados contradicen ampliamente el lugar común que acusa a la religión de ser la principal causa de guerras. No sería la religión la causa de esas guerras, sino el lenguaje que los beligerantes de turno manosearon constantemente para justificar o potenciar el sentimiento de antagonismo entre los pueblos enfrentados y así favorecer intereses políticos o económicos (2009).

3 Con su discurso de las "cuatro libertades", Franklin D. Roosevelt presentó ante el Congreso de los Estados Unidos en 1941 la necesidad de abandonar la posición de neutralidad y combatir contra la Alemania Nazi. Este discurso fue citado en incontables ocasiones por delegados diplomáticos como

expresión se definieron de manera universal hace algunas décadas como una de "las aspiraciones más elevadas" del ser humano (Declaración Universal de Derechos Humanos, preámbulo). Para ajustarnos a la extensión y a la temática de esta publicación, este recorrido histórico sencillo podría fijar aquí el primer estado de la serie de regulaciones sobre lo que hemos denominado blasfemia.[4]

En este estudio observamos que ambas libertades se consagran al mismo nivel y sin preferencia[5]. Sin embargo, la tensión entre ambas libertades no es un fenómeno que tenga un origen jurídico, sino que surge en la convivencia diaria y la regulación jurídica no es capaz de solucionar esa tensión por si sola (como veremos más adelante). En la práctica, la afirmación de una fe suele conllevar a la negación de otras, aunque décadas de estudios teológicos nos demuestren hasta la saciedad que existen mejores formas de convivencia entre personas de diferentes credos (Ratzinger, 2008). Lastimosamente, el mundo en el que vivimos no se caracteriza por la práctica de principios ecuménicos conducentes a la *unitatis redintegratio,* sino por la denigración de quienes mantienen una relación con lo trascendente que difiere de la propia.

Dependiendo del lugar y del momento histórico y de la cercanía de las cicatrices causadas, bien por heridas religiosas o bien por la represión y censura, predominará la regulación jurídica que favorece una u otra libertad. Esto, en cierta medida, no contraviene necesariamente a la igualdad de jerarquía e interdependencia de ambas libertades. Más bien, la regulación que favorece una u otra libertad ha servido como una suerte de acción afirmativa para promover aquella libertad que ha sufrido un inmediato pasado de detrimento. En la Europa de los años 90, cuando la persecución religiosa de los regímenes fascista y socialista todavía era una experiencia

Carlos Rómulo de las Filipinas y por la propia Eleanor Roosevelt durante la redacción de la Declaración Universal de Derechos Humanos para compeler a las potencias vencedoras a incluir la protección de los derechos humanos como uno de los fines principales de la Carta de las Naciones Unidas. Tanta fue la influencia de este discurso de Roosevelt para el nacimiento del derecho internacional de los derechos humanos, que esas cuatro libertades constan recogidas en el segundo párrafo del preámbulo de dicha Declaración Universal: "Considerando que el desconocimiento y el menosprecio de los derechos humanos han originado actos de barbarie ultrajantes para la conciencia de la humanidad, y que se ha proclamado, como la aspiración más elevada del hombre, el advenimiento de un mundo en que los seres humanos, *liberados del temor* y de la *miseria*, disfruten de *la libertad de palabra* y de la *libertad de creencias*;" la cursiva es añadida.

4 Esto sin perjuicio de que existieran otras normas jurídicas nacionales y protointernacionales destacadas en la historia sobre la libertad religiosa y la libertad de expresión como las consagradas en el Cilindro de Ciro (559-529 a. C.). Pero para efectos del razonamiento de este artículo la precisión histórica en el momento y la causa de la regulación, sea de la protección a las creencias religiosas o a la libertad de expresión, no es relevante, ni tampoco es relevante dilucidar qué documento precedió en el tiempo, sino que sin importar el momento de la historia que escojamos, la narrativa de regulación sobre la blasfemia seguirá el mismo curso de colisión y reacción entre la libertad de expresión y la libertad religiosa.

5 No hay que olvidar la interdependencia, la indivisibilidad y la igual jerarquía entre derechos humanos son principios fundantes de esta rama del derecho internacional.

fresca y la tensión en los Balcanes estaba latente para los jueces del Tribunal Europeo de Derechos Humanos, las decisiones de los casos *Wingrove c. el Reino Unido* y *Otto Preminger Institut c. Austria* tendieron a favorecer la libertad de religión por sobre la libertad de expresión. El Tribunal de Estrasburgo prefirió deferir al juicio mejor informado de las autoridades locales sobre las tensiones religiosas que podía causar la proyección de películas blasfemas en cada país, y así justificó la censura de ambas producciones cinematográficas y dijo que mantener tipos penales que castigaban la blasfemia no era, por sí solo, violatorio a los derechos humanos. Mientras que en Latinoamérica, en esa misma década, en la que apenas terminaban las dictaduras censoras y represivas, la Corte Interamericana en *Olmedo Bustos c. Chile* encontró que el mismo tipo de censura judicial a una película ofensiva a la fe cristiana era una violación a la libertad de expresión y, por tanto, no admitiría la censura de ningún tipo. En el caso *Wingrove* se había permitido la censura del filme blasfemo y en *Otto Preminger Institut* se permitió incluso la incautación. Se podría decir que el umbral que la jurisprudencia europea ha marcado y mantenido en decisiones posteriores como *İ.A. c. Turquía* es que las creencias religiosas no pueden estar exentas de crítica a través de diferentes formas de expresión, pero tampoco son permisibles las expresiones ofensivas graves o los "ataques gratuitos" a lo que algunas personas consideran sagrado. Este es un segundo estado de regulación, en el que el derecho tiende a favorecer a aquella libertad que ha sido más afectada en la historia reciente.

El tercer estado es también reaccionario y se puede apreciar mejor en las repercusiones tras las decisiones del Tribunal Europeo. Organizaciones internacionales y la sociedad civil emprendieron una fuerte campaña para que en el Reino Unido se despenalizara la blasfemia porque se consideraba ese tipo penal como una violación a la libertad de expresión. Desde 1999, el Relator Especial de las Naciones Unidas sobre Libertad de Opinión y Expresión, el Representante de la OSCE sobre Libertad de los Medios y el Relator Especial de la OEA para la Libertad de Expresión han emitido declaraciones conjuntas instando a que las leyes penales contra la blasfemia sean derogadas, para garantizar el libre flujo de opiniones, incluso de aquellas que puedan considerarse ofensivas y así garantizar un debate abierto sobre cuestiones de interés público.

Es cierto que en casos como el de *Otto Preminger Institut* la censura y confiscación de una película blasfema estuvo orientada a proteger de un ataque gratuito a las personas sagradas para el 90% de la población de la pequeña ciudad austriaca de Tirol. Pero también es cierto que en muchos otros lugares, las leyes de blasfemia cumplen cualquier propósito represivo, menos el de proteger el sentido de lo sacro. En lugares como Argelia sirven como excusa para el asesinato de periodistas que denuncian actos de violencia o corrupción de grupos religiosos extremistas; en Somalia y Canadá, bajo la acusación de blasfemia, se ha perseguido a religiosos reformistas; en Tayikistán se apresó a periodistas que entrevistaron a facciones acusadas oficialmente de sostener visiones religiosas inaceptables. Se

podrían citar otros ejemplos más comunes de asesinatos selectivos de periodistas y de ejecuciones de minorías religiosas o de persecución a disidentes políticos, todo justificado como blasfemia desde Afganistán o Arabia Saudita hasta Mali o Marruecos (Marthoz, 2013). Incluso en el Reino Unido, cuando se discutía en 2008 la derogatoria del tipo penal de la blasfemia, el propio Arzobispo de Canterbury manifestó su apoyo a esa reforma legal, pues la historia inglesa tampoco estuvo libre de persecución y represión enmascarada por una supuesta protección a los sentimientos religiosos.

En el Ecuador, la trayectoria de regulación es la misma. Desde la Constitución de 1830 se garantizaba que "todo ciudadano puede expresar y publicar libremente sus pensamientos" (artículo 64) y proclamaba la protección de la religión de manera confesional (artículo 8). Consecuentemente, el Código Penal de 1837 sancionaba a quien "ultrajare o escarneciere los objetos consagrados al culto religioso, en los templos o lugares destinados a su ejercicio" (artículo 140). El mismo modelo siguieron las constituciones de 1835 hasta la de 1897, pero en la Constitución liberal de 1906 el péndulo osciló hacia la eliminación de toda mención de la religión en la Constitución, como respuesta a las restricciones que habría impuesto el modelo confesional de las constituciones anteriores. Este modelo se mantuvo solamente en la Constitución de 1929; en 1945, la Constitución adoptó una versión más cercana a la libertad religiosa que conocemos en el presente bajo la fórmula "El Estado no reconoce religión oficial alguna. Todos pueden profesar la que a bien tengan" (artículo 141.11). Como es de esperar, la legislación penal siguió la misma suerte que la Constitución. El Código Penal publicado el 18 de abril de 1906 ya no penaba la difamación de la religión y esta no volvió a ser tipificada, como tampoco el código de 1938, ni en las codificaciones de 1960 y posteriores. Es así como el Ecuador se quedó con un modelo de protección constitucional de ambas libertades siguiendo, en líneas generales, las tendencias del derecho internacional de los derechos humanos.

Esto no quiere decir que la protección de los lugares sagrados, de los símbolos religiosos y de las personalidades veneradas en diferentes religiones haya dejado de ser una parte fundamental de la libertad de religión. A nivel internacional, al mismo tiempo que los relatores especiales sobre libertad de expresión continuaron emitiendo declaraciones conjuntas en 2000 y 2002, el Consejo de Derechos Humanos de las Naciones Unidas "observa[ba] con profunda preocupación la intensificación de la campaña general de difamación de las religiones y la incitación al odio religioso", y "deplora[ba] el uso de la prensa [...], incluido el internet, [...] para incitar a cometer actos de violencia, xenofobia o formas conexas de intolerancia y discriminación contra cualquier religión, así como para atacar símbolos religiosos y personas veneradas" (Resolución 10/22, 2009, pp. 2-3).

El reconocimiento de las dos libertades interdependientes y con un mismo nivel de importancia no basta para proteger a las personas contra la represión y censura arbitraria, ni contra la difamación de sus religiones. La prohibición y la regulación

jurídica no han sido mecanismos suficientes para contener la ofensa a las relaciones más allegadas y trascendentales del ser humano, no se trata de un problema que se pueda solucionar solamente tratando de encontrar la medida justa de regulación o desregulación.

3. Las respuestas incompletas en el Derecho

La tendencia actual, marcada por las declaraciones conjuntas de los relatores especiales y confirmada en los Comentarios Generales del Comité de Derechos Humanos que vigila la implementación del Pacto Internacional de Derechos Civiles y Políticos, es que ninguna expresión debe estar prohibida y menos aún penalizada (CCPR/C/GC/34, 2011, párr. 48). Según las declaraciones conjuntas de los relatores especiales, lo único permisible serían las regulaciones mínimas de derecho privado que no representen censura ni sanción para la emisión de cualquier tipo de expresiones, sino solamente la justa reparación a la difamación en la que se pueda haber incurrido.

Fuera del lenguaje oficial de las declaraciones conjuntas, la anterior Relatora Especial de la OEA para la Libertad de Expresión, Catalina Botero, ha explicado de manera más informal en una entrevista con El Universo en 2008 el razonamiento que inspiran los documentos oficiales. Para Botero "las ideas y las creencias no tienen honra" de tal forma que no se puede ofender a una idea. Ella piensa (y como veíamos en párrafos anteriores, con mucha razón) que con "la prohibición de la blasfemia lo que logran [los gobernantes] es evitar el debate sobre la forma como ellos ejercen el poder." Por eso, lo único que sería posible prohibir, según el derecho internacional de los derechos humanos, es la incitación expresa e inmediata a la violencia, pero insultar o blasfemar no serían una incitación de ese tipo.

Esta lectura de Botero de los artículos 13 de la Convención Americana sobre Derechos Humanos y de los artículos 19 y 20 del Pacto Internacional de Derechos Civiles y Políticos, con seguridad, es bienintencionada y está orientada a la promoción de un debate público vigoroso, pero sufre de una ingenuidad nociva. Los relatores especiales, con sus años de experiencia, y por el tipo de trabajo que realizan, seguramente han desarrollado la capacidad de recibir agravios contra ellos, sus familias, sus creencias u orientaciones políticas sin caer en la tentación de responder a la provocación, pero sería extremadamente ingenuo pensar que todos reaccionan con la misma moderación frente al agravio. El mundo no está hecho solamente de relatores especiales, un mundo tan uniforme es imposible y mucho menos deseable. En la infinidad de culturas y personalidades que dan color a nuestro mundo, todos reaccionamos al agravio de manera diferente y también cambiamos con la edad, la educación y las circunstancias que en un determinado momento nos confortan o nos agobian. Frente al agravio y a la provocación existe y existirá siempre la posibilidad del resentimiento y también la posibilidad de reacción, hasta llegar a la retaliación, aunque preferiríamos pensar que nuestra reacción siempre será sobria.

Lastimosamente, la interpretación predominante del marco normativo internacional se ha construido con esa ingenuidad. Al estado actual de desregulación en la protección de la libertad de religión le acompaña un discurso de libertad de expresión casi absoluta, sin posibilidades de limitación previa, sino solamente con el reconocimiento de responsabilidades ulteriores, salvo en el caso extremo de incitaciones inmediatas a la violencia. Estos movimientos oscilatorios extremos entre la regulación (en forma de penalización) y la desregulación (a manera de despenalización) solamente demuestran la incapacidad de las prohibiciones para dar respuesta por sí solas a la problemática y rica relación de interdependencia entre seres humanos y sus derechos.

La única forma de que las libertades que tienden a colisionar convivan con tensiones, pero sin escalar a vejámenes, es con la renovación constante del compromiso de ejercer la libertad como un decidir, obrar y expresar lo que contribuye a mi bien personal y reconocer que nada será bueno para mí si le causa deliberadamente el mal otro e incluso si le causa el mal como consecuencia indirecta, pero previsible (como lo demuestran las discusiones filosóficas sobre lo que constituye el bien común) (Jeffery, 2015). En este tema, la jurisprudencia del Tribunal Europeo de Derechos Humanos ha sido mucho más acertada, y su respuesta regulatoria ha sido mucho más elocuente que los extremos de penalización y despenalización, ya que ha considerado en el debate que la ofensa grave o el ataque gratuito no son formas de alcanzar ningún bien para el que las profiere y no se justifican de ninguna manera en el discurso del derecho internacional de los derechos humanos que busca defender las "aspiraciones más elevadas de la humanidad" y no las más bajas.

Por supuesto que es muy complicado determinar qué insulta y qué constituye una crítica legítima, qué es blasfemo y qué es un cuestionamiento válido a la fe de otro, pero que esto sea difícil no quiere decir que no debamos hacerlo. El Tribunal Europeo ha puesto a disposición de estos debates complicados la institución jurídica del margen de apreciación y así ha logrado aproximarse a mejores respuestas que se compadecen de las circunstancias particulares de cada caso, para no caer en la ingenuidad de emitir una sola fórmula abstracta y también ambigua para resolver el problema, como lo hacen otros actores internacionales al admitir únicamente la prohibición de lo que incita inmediata e inequívocamente al odio y la violencia, pues la definición de estos últimos cuatro términos tampoco es sencilla.

Ninguno de los relatores especiales estaría dispuesto a reconocer que las caricaturas del periódico danés Jyllands-Posten de 2005 o las más recientes de Charlie Hebdo incitaban al odio o a la violencia. Más bien, es común entre los intelectuales del derecho y los formadores de opinión pública sostener, como Botero, que todas las personas deben estar dispuestas a ridiculizar y ser ridiculizadas para ingresar al libre mercado de las ideas, donde se debaten las prerrogativas, políticas públicas y leyes que se aplicarán a cada comunidad en todo gobierno legítimo y democrático de cualquier Estado contemporáneo (Dworkin, 2006).

Sin importar cuántas columnas editoriales repitan ese mismo credo de la democracia liberal, ni cuántas resoluciones se emitan en el mismo sentido desde Ginebra, Nueva York o Washington, cada aniversario de las ejecuciones y atentados no podremos dejar de preguntarnos qué más se podría haber hecho para prevenir esas tragedias y qué se podría hacer para prevenir otras similares. Será un síntoma de que continuamos fallando si continuamos presenciando cómo jóvenes ofendidos en sus creencias (o que no encuentran espacio para expresarlas en un ambiente de respeto) siguen recurriendo a la alternativa de la radicalización en grupos que capitalizan este ambiente hostil contra la religión para justificar sus actos de terror.

La respuesta regulatoria más adecuada la conocemos desde 1948: todos los derechos humanos son limitados, ninguno es absoluto, el mismo derecho a la vida admite excepciones en la legítima defensa y en las normas sobre la conducción de conflictos armados, así como del uso progresivo de la fuerza por fuerzas de seguridad en tiempo de paz, sin necesidad de entrar en ejemplos éticamente complejos como la pena de muerte. Las limitaciones a los derechos humanos no son obstáculos a salvar, sino bienes que hay que defender como expresión de la interdependencia de las necesidades personales, cuya satisfacción fraccionada conduce a una vida de frustración e insatisfacción, a las que solo se les puede hacer justicia con una visión integral de la persona, teniendo en cuenta la interdependencia de sus propias necesidades y la interdependencia entre seres humanos (Glendon, 1991, pp. 18 *et seq*).

En resumen, el derecho nos aporta dos respuestas sobre la riqueza de alternativas que pueden potenciar la realización de ambos derechos en cuestión a través de la regulación. En primer lugar, la regulación jurídica permite materializar el principio de subsidiaridad[6] a través de instituciones como el margen de apreciación, para que las autoridades no tengan que asumir con soberbia que ellas solas pueden deducir en abstracto y de manera general qué constituye una expresión nociva, qué es una crítica y qué es una ofensa, sino que puedan deferir las prácticas de cada comunidad y entender los valores que ellas cultivan antes de tomar una decisión. La segunda respuesta que puede aportar el derecho es llevar a la práctica las limitaciones de los derechos humanos que son la manifestación, por excelencia, del principio de interdependencia que potencia el florecimiento humano, no lo restringe.

---

6 “La subsidiariedad [es un principio estructural que] expresa una concepción del hombre, de la sociedad, [del derecho] y del universo. Como principio de organización social incluye primero una prohibición: todo lo que cada uno puede realizar por sí mismo y con sus propias fuerzas no debe ser transferido a otro nivel [de organización social]. Pero tiene sobre todo un sentido positivo: cuando la capacidad de una acción comunitaria se revela insuficiente no debe ser tomada a cargo automáticamente dentro de una comunidad más amplia. Al contrario, esta comunidad más amplia deberá ayudar y sostener a la comunidad deficiente. Desde su nivel superior debe restaurar la capacidad de acción de la comunidad que resulta momentáneamente insuficiente (McCadden, 1992).”

La pregunta central sale de la esfera de lo puramente jurídico: ¿cuáles son las limitaciones necesarias a la libertad de expresión y, en este caso, al internet y a los derechos digitales para respetar otros derechos, como por ejemplo las libertades religiosas? La respuesta no puede ser automática, como es la tendencia actual del derecho internacional de los derechos humanos y que se puede observar en el caso *Olmedo Bustos c. Chile* y en las declaraciones conjuntas de los relatores especiales sobre libertad de expresión. Si en el internet seguimos la lógica reducida de oscilaciones extremas entre prohibición y eliminación de la prohibición, veremos que el ejercicio de libertades de comercio, empresa, expresión, etc., serán disminuidas para favorecer temporalmente consideraciones (que pueden ser muy legítimas) sobre seguridad y protección especial, pero esa forma de regulación continuará sin dar una solución de fondo a problemas graves y será solamente cuestión de tiempo hasta que haya una reacción que recupere el espacio perdido de las libertades y sacrifique los intereses legítimos de seguridad y protección. Las posibilidades de regulación son mucho más amplias y favorables que la sola prohibición y sanción, y cualquier forma de regulación efectiva que se escoja debe servir para promover (y no silenciar artificialmente) discusiones éticas sobre qué constituye un buen uso de espacios como el internet y cómo alcanzar el bien común en el ejercicio de nuestros derechos y libertades.

4. Virtud, educación y libertad

No basta, como comenta Joseph Weiler a propósito de la Unión Europea, contar con un marco normativo que defienda ideales altos como los que se plasmaron en el Convenio Europeo de Derechos Humanos, si su aplicación en la cotidianeidad, tanto por los ciudadanos europeos, como por sus autoridades, no persiguen esos ideales de justicia y libertad con virtud personal en la práctica (2009, pp. 56-58). La Unión Europea suponía el valor de la protección de la persona y sus derechos fundamentales, pero ha resultado en la protección y promoción de un individuo egocéntrico que, en lugar de buscar la prosperidad y el bienestar económico para gozar de una existencia digna (que incluya la práctica de la solidaridad), ha incentivado el materialismo egoísta en un sistema político cuyos actores no están dispuestos a asumir sus responsabilidades frente a la democracia, desde el Consejo de Europa, pasando por los gobiernos nacionales, hasta llegar a cada uno de los ciudadanos (pp. 58-69). Weiler presenta variados ejemplos sobre cómo la Unión Europea se ha convertido en una víctima de sus elevados ideales implementados de manera viciada por y para un individuo denigrado.

Este doble objetivo de promover sujetos de derechos que busquen los ideales de dignidad y ejerzan su libertad con virtud es muy simple de enunciar, pero mucho más complicado de llevar a la práctica porque no es algo que el derecho pueda solucionar directamente a través de la prohibición o sanción. “Si el verdadero problema es volver a despertar, regenerar la persona, entonces el lugar recóndito donde la persona puede ser rescatada no es ni un discurso ni un debate” (Carrón, 2015, p. 46), mucho menos un debate jurídico.

Para aprender hasta dónde reclamar respeto hacia los sentimientos religiosos ofendidos por expresiones blasfemas o para reconocer hasta dónde pueden extenderse las expresiones de quienes usan el internet como medio para difundir diferentes ideas, hace falta concentrarse en la educación. Quienes practicamos, estudiamos o elaboramos el derecho no debemos perder de vista que muchos de los temas más acuciantes que invitan a la regulación del internet no pueden ser resueltos mediante prohibiciones que, especialmente en el espacio digital, presentan desafíos grandes para su implementación, para la identificación de responsables, su enjuiciamiento y la posterior sanción en jurisdicciones transnacionales.

La generación de un sujeto de derechos responsable, o de un sujeto capaz de juzgar con razonabilidad práctica sus acciones y decisiones, no se da por decreto legislativo, sino que se genera a través de la educación a la libertad (ver Glendon, 1991). Sin sujetos responsables, todas nuestras discusiones sobre regulación y desregulación, tanto en el ámbito del internet como fuera de él, van a carecer de profundidad y serán solamente la imposición normativa del dogma político de la mayoría de turno (ver Hand, 1952, pp. 189-190). Debemos aspirar a que nuestro marco normativo favorezca, o por lo menos no obstaculice, discusiones éticas y políticas profundas. Al Derecho no le corresponde directamente generar la responsabilidad y la ética en los sujetos de derechos humanos, pero el Derecho sí puede contribuir decisivamente al menos de dos maneras: garantizando que el marco normativo internacional, constitucional y legal favorezca y nunca disminuya la libertad de educación y (a propósito de blasfemia) protegiendo la libertad de asociación y religión para que iglesias, comunidades religiosas y sus asociaciones tengan espacio para propagar los valores y las virtudes que son consubstanciales a su existencia y que sirven de límite verdadero al abuso de derechos y libertades (Carozza, 2012, pp. 202-203; Garnett, 2010, pp. 267-281).

Bibliografía:

Carozza, P. (2012). “Religión, libertad religiosa y derechos humanos” en Traslosheros, J. (coord.), *Libertad Religiosa y Estado Laico.* México: Editorial Porrúa, pp.189-203.

Carrón, J. (2015). *Una presencia en la mirada,* Suplemento de la revista Huellas - Litterae Communionis, n. 6, junio de 2015.

Corte Interamericana de Derechos Humanos (2001). Caso Olmedo Bustos y otros) c. Chile.

Finnis, J. (2011). *Natural Law and Natural Rights.* New York: Oxford University Press.

Garnett, R. (2010). “Religious liberty, church autonomy, and the structure of freedom” en Witte, J. et al (eds.), *Christianity and Human Rights*, New York: Cambridge University Press, pp. 267-281.

Glendon, M.A. (1991). *Rights Talk: The Impoverishment of Political Discourse.* New York: Free Press.

Hand, L. (1952). *The Spirit of Liberty: Papers and Addresses of Learned Hand,* New York: Knopf.

Human Rights Committee. (2011), General Comment No. 34, CCPR/C/GC/34.

Keogh, D. (1981). *Romero, El Salvador's Martyr: A Study of the Tragedy of El Salvador*. Dublin: Dominican Publications.

Lawrence, L. (1999). *Code: and other laws of cyberspace.* New York: Basic Books.

Lawrence, L. (2001). *The future of ideas: the fate of the commons in a connected world.* New York: Random House.

Lawrence, L. (2006). *Code: and other laws of cyberspace, version 2.0*. New York: Basic Books.

Marthoz, JP. (2013). "Extremists are Censoring the Story of Religion", *Committee to Protect Journalists*, < https://cpj.org/2013/02/attacks-on-the-press-journalism-and-religion.php >, [07/21/2016].

McCadden, C. (1992) "El principio de subsidiariedad y el Tratado de Maastricht", *ITAM* <http://biblioteca.itam.mx/estudios/estudio/letras30/notas2/sec_1.html>, [07/21/2016].

Meierhenrich, J. (2014). *Genocide: a reader.* New York: Oxford University Press.

Meyer, J. (2013) *La Cristiada: The Mexican People's War for Religious Liberty*. New York: Square One Publishers.

Nicholas, Jeffery L. (2015) "The Common Good, Rights, and Catholic Social Thought: Prolegomena to Any Future Account of Common Goods," *Solidarity: The Journal of Catholic Social Thought and Secular Ethics*: Vol. 5: Iss. 1, Article 4.

Ratzinger J. (2008). *Church, Ecumenism and Politics: New Endeavors in Ecclesiology*. San Francisco: Ignatius Press.

Traslosheros J. (2012), *Libertad religiosa y Estado laico. Voces, fundamentos y realidades*, México: Editorial Porrúa.

Tribunal Europeo de Derechos Humanos. (1994). Otto-Preminger-Institut c. Austria.

Tribunal Europeo de Derechos Humanos. (1995). Wingrove c. Reino Unido.

Tribunal Europeo de Derechos Humanos. (2005). İ.A. c. Turquía.

Weiler, J. (2009). "Europa: Nous coalisons des etats, nous n'unissons pas des hommes" en Cartabia, C, e Simoncini, A. (eds), *La sostenibilità della democracia nel XXI secolo.* Bologna: Società Editrice il Mulino.

Respuesta administrativa a los derechos sociales, especial énfasis en las tecnologías disruptivas

Javier Robalino Orellana
Universidad San Francisco de Quito

RESUMEN: Parte fundamental de la regulación de internet recae en la complejidad con la que se reglamenta las tecnologías disruptivas y cómo ello afecta a la economía digital.

PALABRAS CLAVE: tecnologías disruptivas, internet, economía digital, derechos digitales, intermediarios de internet, derechos humanos.

ABSTRACT: A fundamental part of internet regulation lies in the complexity with which disruptive technologies is regulated and how this affects the digital economy.

KEYWORDS: disruptive technologies, internet, digital economy, digital rights, internet intermediaries, human rights.

1. Introducción

El término Tecnologías Disruptivas fue acuñado, por primera vez, por Clayton Christensen, en una publicación denominada "El dilema del innovador"[1]. En esta publicación se utilizó este término para describir a aquellas innovaciones que crean nuevos mercados, descubriendo nuevas categorías de consumidores. Así, estos nuevos agentes crean el mercado utilizando las nuevas tecnologías, pero también los nuevos modelos de negocios que, a su vez, les permiten explotar las viejas tecnologías en nuevas formas.

Sin embargo, a pesar de la prolongada existencia de la teoría de la disrupción, no ha sido entendida en su totalidad. A menudo, se utiliza el término solamente para hablar de la innovación o para atraer más consumidores, pero esta teoría se refiere a una nueva tecnología que presenta menores costos y un mejor performance.

Lo que se pretende en este artículo es ver la respuesta y las obligaciones estatales con relación a las nuevas tecnologías disruptivas, tomando en cuenta los derechos humanos y constitucionales que han sido garantizados por el propio Estado a sus ciudadanos.

2. Tecnologías Disruptivas

El término Tecnologías Disruptivas cada vez es más común, sin embargo, no siempre se lo utiliza adecuadamente, lo que genera un desconocimiento y una confusión cada vez mayor. De esta forma, en primer lugar, se debe definir este término, para, posteriormente, determinar las características que deben ocurrir para que un determinado negocio sea considerado de esta forma.

Así, se ha entendido como una innovación disruptiva al proceso por el cual un producto o un servicio tienen, como inicio, una simple aplicación en el fondo del mercado, el cual, implacablemente, va ascendiendo y, eventualmente, desplaza a los competidores establecidos[2]. Mediante este tipo de tecnologías se permite que la población tenga acceso a un producto o servicio que históricamente era una posibilidad solo para los consumidores con mucho dinero.

Sin embargo, un negocio o una innovación disruptiva en sus etapas o fases iniciales pueden incluir un margen de ganancia menor, mercados más pequeños y productos o servicios más simples que, en un inicio, podrían no ser tan atractivos como aquellos ya existentes. Es justamente por las pocas ganancias que generan en

---

1 El libro fue publicado en 1997 en Harvard Business School Press. El título completo del mismo fue "The Innovator's Dilemma; How New Technologies Cause Great Firms to Fail".

2 Traducción del original: "Disruptive innovation, a term of art coined by Clayton Christensen, describes a process by which a product or service takes root initially in simple applications at the bottom of a market and then relentlessly moves up market, eventually displacing established competitors" Clayton Christensen. *Disruptive Innovation*. http://www.claytonchristensen.com/key-concepts/#sthash.ExiY5YaI.dpuf

un principio, lo que les vuelve poco atractivas para aquellas compañías o agentes del mercado, con lo cual se genera un lugar para los competidores disruptivos, para que emerjan desde el fondo del mercado[3].

Por lo mencionado, podemos decir que las innovaciones o tecnologías disruptivas son un proceso mediante el cual una compañía con pocos recursos puede competir efectivamente con los negocios ya establecidos. Así, buscan mejorar los productos y servicios para los consumidores más exigentes, quienes, a su vez, son los que más ganancias generan, por lo que sus necesidades se visibilizan más, mientras que, las de los otros grupos, se ignoran. De esta forma, los agentes disruptivos inician exitosamente en aquellos segmentos del mercado que han sido pasados por alto por los otros competidores, estableciéndose en el mercado por entregar bienes o servicios más adaptados a las necesidades o demandas de los consumidores con menores precios, por lo tanto, aquellos agentes ya establecidos, que adicionalmente buscan mayores beneficios, no responden a la entrada en el mercado, pues no suponen una amenaza para ellos. Esta actitud de los grandes agentes permite que el disruptivo vaya subiendo en el mercado, con las prestaciones que los consumidores requieren y que se genere, así, una ventaja en el mercado por la innovación presentada al iniciar sus actividades. Por lo tanto, cuando los agentes establecidos empiezan a modificar su conducta y a ofrecer los bienes o servicios, de la forma o con la calidad similar a la que realiza el nuevo agente en el mercado, la disrupción se ha producido.

Según el creador de esta teoría, para determinar si una innovación es realmente disruptiva o no, se deben cumplir ciertas características. La primera de estas características es que una innovación disruptiva se genera en un mercado pequeño o nuevo[4]. Esta característica establece que las innovaciones deben aparecer en este tipo de mercados que son los que han sido pasados por alto por los agentes establecidos. Los mercados pequeños se generan, debido a que los agentes ya establecidos buscan satisfacer las necesidades de los consumidores más exigentes, mejorando sus bienes o servicios para complacer tales necesidades, eso hace que se preste menos atención a los demás consumidores. Esta situación, a su vez, genera una oportunidad para los agentes disruptivos, puesto que desde un inicio estos se enfocan en proveer a aquellos consumidores ignorados de un producto o servicio lo suficientemente bueno.

Por un lado, en el caso de nuevos mercados, los agentes disruptivos crean uno que anteriormente no existía. Dicho de otra forma, convierten en consumidores a aquellas personas que antes no lo eran.

---

3 Disruptive Innovation. Clayton Christensen. http://www.claytonchristensen.com/key-concepts/#sthash.ExiY5YaI.dpuf

4 Clayton Christensen, Michael Raynor y Rory Macdonald. "What is disruptive innovation?" *Harvard Business Review* (2015), pág. 47.

Por lo mencionado, se debe entender que la Teoría de la Disrupción establece que las innovaciones disruptivas son diferentes de las denominadas innovaciones de sostenimiento, las cuales mejoran los productos o servicios existentes de los agentes establecidos, como, por ejemplo, la imagen más nítida en la televisión o la mejora en la cobertura de telefonía celular[5]. Estas mejoras son avances significativos que permiten a las empresas vender más productos a sus clientes más rentables.

Por otro lado, las innovaciones disruptivas son consideradas como inferiores o insignificanticas por la mayoría de los consumidores de los agentes establecidos. Esto debido a que los consumidores no están dispuestos a cambiarse al nuevo bien o servicio establecido solo porque es más barato, por el contrario, esperan a que la calidad mejore lo suficiente como para satisfacer sus expectativas. Una vez que esto sucede, se cambian al nuevo producto ofrecido, en el que, además, aceptan el menor costo que este representa; así es como las innovaciones disruptivas bajan los precios en el mercado.

Adicional a lo ya establecido, se debe mencionar que existen cuatro puntos importantes que son mal entendidos o pasados por alto. El primero de ellos es que la disrupción es un proceso. Esto es importante analizar, puesto que el término ha sido mal utilizado, ya que, muchas veces, el mismo ha sido utilizado para referirse a un producto o servicio en un punto determinado, más que a la evolución del mismo en el tiempo. Es así que la mayoría de innovaciones, sean disruptivas o no, son pequeñas en su inicio. Por lo tanto, los agentes disruptivos tienden a enfocarse en el modelo del negocio, más que en el producto en un primer momento, puesto que una vez que puedan crecer, comparten con los negocios establecidos, no solamente su parte en el mercado, sino también sus ganancias. Obviamente, este proceso puede tardar un tiempo, ya que si el producto innovador adquiere una ventaja, los agentes establecidos pueden defender acérrimamente su posición en el mercado.

El segundo y tercer punto explican que los agentes disruptivos, a menudo, crean o generan modelos de negocios que son muy diferentes a los agentes establecidos y que no todas las innovaciones disruptivas siempre tienen éxito. Esto último quiere decir que una compañía o agente es disruptiva por el nivel de éxito que haya alcanzado.

El cuarto punto al que se hace referencia es que el lema "perturbar o ser perturbado" puede ser engañoso. La aparición de las compañías disruptivas puede generar un cambio en el comportamiento de los agentes establecidos en el mercado, los cuales deben responder a la disrupción, pero no desmantelar un modelo que aún es rentable. Por el contrario, los agentes establecidos deberían mejorar las relaciones con sus consumidores e invertir en innovaciones sustanciales. Con respecto a

---

5 Clayton Christensen, Michael Raynor y Rory Macdonald. "What is disruptive innovation?" *Harvard Business Review* (2015), pág. 47.

lo mencionado, la teoría de la disrupción predice que cuando un nuevo agente entra al mercado ofreciendo mejores productos o servicios, los agentes establecidos invierten y aceleran las innovaciones en sus negocios, por lo tanto, o contratacarán ofreciendo aún mejores bienes o servicios en precios comparables o comprarán al agente entrante[6].

Por lo tanto, como ejemplo de innovaciones disruptivas típicamente se menciona a las laptops o computadoras personales, las cuales, en su momento, crearon un enorme y nuevo mercado, puesto que previo a su aparición, las computadoras de escritorio eran vendidas únicamente a grandes corporaciones o universidades de investigación. Otro ejemplo es Xerox, con la tecnología del fotocopiado, la cual apuntó a las grandes corporaciones y redujo los altos costos que estas operaciones presuponían.

En la actualidad, existe un debate sobre si Uber consiste en una innovación disruptiva o no. Si bien existen las dos posiciones, los creadores de esta teoría se han decantado diciendo que este servicio no constituye una innovación disruptiva, a pesar de utilizar de buena manera las ventajas tecnológicas: en primer lugar, debido a que esta plataforma no se originó en un pequeño o nuevo mercado, sino en uno bien establecido como es el de los taxis. En este sentido, el negocio de Uber ha ido a la inversa de lo establecido por la teoría, la cual indica que los nuevos agentes deben generarse desde los espacios de los mercados desatendidos o inexistentes; sin embargo, esta plataforma empezó con el mercado principal y se ha ido expendiendo poco a poco hacia los sectores históricamente desatendidos. Por lo tanto, los logros que esta plataforma ha obtenido se deben al desarrollo tecnológico, lo que ha permitido brindar un servicio menos costoso y satisfacer, de mejor manera, las necesidades de los consumidores.

Al contrario, Netflix presupone un buen ejemplo de innovación disruptiva, puesto que, en sus inicios, la plataforma no estaba destinada a competir contra las grandes cadenas de alquiler de películas como Blockbusters, por el contrario, estaba enfocada a pequeños grupos de consumidores que no necesariamente estaban interesados en los estrenos, puesto que en un principio esta plataforma no contaba con ese servicio, mientras que las grandes cadenas sí. Sin embargo, lentamente esta aplicación fue creciendo cada vez más, por la ventaja que había obtenido a la pionera en el mercado, entregando a los consumidores de las grandes cadenas un servicio con mayor contenido, con un menor precio y de mejor calidad, lo que causó que eventualmente Blockbuster haya colapsado[7].

Recapitulando lo antes mencionado, las innovaciones disruptivas usualmente encuentran consumidores en mercados pequeños o inexistentes, lo que hace que

---

6 Clayton Christensen, Michael Raynor y Rory Macdonald. “What is disruptive innovation?” *Harvard Business Review* (2015), pág. 51.

7 Nathan McAlone. “The father of ‘disruption’ theory explains why Netflix is the perfect example — and Uber isn’t”. Business Insider (2005).

los agentes establecidos lentamente reconozcan las amenazas que estos representan, sin embargo, conforme crecen, terminan redefiniendo y cambiando mercados enteros. Por lo tanto, podemos decir que se entienden a las nuevas tecnologías como mecanismos mediante los cuales se crea valor agregado y nuevas interacciones, generalmente a través de plataformas tecnológicas o aplicaciones diseñadas para dispositivos móviles o teléfonos inteligentes. Así, se define a las tecnologías disruptivas como aquellas que alteran, de forma significativa, la manera en la cual operan los negocios y la sociedad en general. Esta clase de tecnología obliga a los negocios y a los distintos agentes económicos que operan en el mercado a alterar su comportamiento, para adaptarse a los cambios tecnológicos y así evitar volverse obsoletos.

3. Rol del Estado

Una vez analizado el concepto de tecnologías o innovaciones disruptivas, es necesario analizar la respuesta estatal frente al auge, cada vez mayor, de este tipo de negocios. Por lo tanto, deben existir respuestas por parte de las autoridades que no solamente protejan estas innovaciones, sino también que las promuevan, puesto que la participación del Estado se consolida y forma parte del proceso de transformación productiva, generando eficiencias y aprovechamiento de los avances tecnológicos.

De esta forma, la regulación busca corregir las deficiencias que presenta el mercado, lo que implica establecer normas generales de comportamiento económico. Esto, en general, es una respuesta *ad hoc* a los eventos económicos o a la percepción de las fallas del mercado por parte del Estado.

Con relación a lo mencionado, las normas generales de comportamiento son un conjunto de reglas generales y específicas impuestas por las agencias de regulación del Estado que interfieren directamente en el mecanismo de asignación del mercado o indirectamente cuando alteran las decisiones de oferta y demanda de los usuarios y de las empresas prestadoras de servicios u oferentes de bienes.

Por su lado, el concepto de fallos del mercado, a su vez, se refiere a una situación en la que un determinado mercado no organiza eficientemente la producción o la asignación de los bienes y servicios para los consumidores. Ejemplos de fallos de mercado son: la competencia imperfecta, las asimetrías de la información y el problema de riesgo moral.

Frente a lo mencionado, se debe realizar un análisis sobre el costo beneficio de la regulación. En este sentido, el Estado debe aproximarse a las tecnologías disruptivas desde una perspectiva económica y reconocer que existen fallos del mercado que generan externalidades negativas, por lo que cabe la intervención del Estado cuando se verifica este supuesto, cuando se constata un perjuicio al consumido o una práctica de competencia desleal. Dado que también existen fallas en la regu-

lación de una actividad, se debe emplear la teoría económica para comparar los costos y la pérdida de utilidad que un cambio de regulación implica para diferentes miembros de la sociedad.

Sin embargo, se deben considerar ciertos factores al momento de regular tecnologías disruptivas. En este sentido, es fundamental mencionar que la regulación en cuestión no debe frenar la innovación, sino, por el contrario, debe demostrar que la regulación genera un beneficio al consumidor y no solamente a grupos económicos de poder que se encuentran atrás de los oferentes que promueven la regulación. El Estado también debe tomar en cuenta, al momento de la regulación, las posibles afectaciones que se pueden generar en contra de los negocios crecientes, en cuanto a los derechos consagrados, no solamente en el ordenamiento jurídico nacional, sino también en los diversos instrumentos internacionales, sobre todo en aquellos relacionados a los derechos humanos, los cuales se analizarán en la siguiente sección.

4. Derechos Humanos

El tema en cuestión está íntimamente ligado con los derechos fundamentales de las personas. En este y el siguiente capítulo, no se pretende dar definiciones de los derechos a los que se hará referencia, sino, justamente, se analizarán los derechos que están íntimamente involucrados con el tema de la presente investigación. También es importante mencionar que a pesar de que posteriormente se hará un análisis de los derechos constitucionales, los derechos humanos según la Constitución del Ecuador tienen una jerarquía superior[8], por lo tanto, se analizarán los mismos en primer lugar, para luego tratar los derechos reconocidos en el ordenamiento jurídico local.

Los derechos humanos también tienen especial importancia y relevancia en el ordenamiento jurídico ecuatoriano, en virtud de las disposiciones contenidas en la Constitución, las cuales mandan que en el caso de los tratados y otros instrumen-

---

8 La Constitución de la República del Ecuador establece un orden jerárquico de aplicación de las normas, el cual se determina en los artículos 424 y 425, los cuales mandan que la “La Constitución es la norma suprema y prevalece sobre cualquier otra del ordenamiento jurídico. Las normas y los actos del poder público deberán mantener conformidad con las disposiciones constitucionales; en caso contrario carecerán de eficacia jurídica. La Constitución y los tratados internacionales de derechos humanos ratificados por el Estado que reconozcan derechos más favorables a los contenidos en la Constitución, prevalecerán sobre cualquier otra norma jurídica o acto del poder público”. En cuanto a la aplicación determina que “El orden jerárquico de aplicación de las normas será el siguiente: La Constitución; los tratados y convenios internacionales; las leyes orgánicas; las leyes ordinarias; las normas regionales y las ordenanzas distritales; los decretos y reglamentos; las ordenanzas; los acuerdos y las resoluciones; y los demás actos y decisiones de los poderes públicos”.
Por lo tanto, se evidencia claramente que la Constitución y los Tratados internacionales son las normas de primera aplicación, haciendo una puntualización con relación a los instrumentos internacionales de derechos humanos, los cuales según la redacción de la norma, tienen un rango supra constitucional siempre y cuando reconozcan derechos más favorables a los establecidos en la Norma jerárquicamente superior.

tos internacionales de derechos humanos se aplicarán los principios pro ser humano, de no restricción de derechos, de aplicabilidad directa y de cláusula abierta establecidos, todos presentes en la Constitución. En el mismo sentido, la norma establece que los derechos y las garantías establecidos en la Constitución y en los instrumentos internacionales de derechos humanos serán de directa e inmediata aplicación por y ante cualquier servidora o servidor público, administrativo o judicial, de oficio o a petición de parte[9].

En este análisis, debemos mencionar que los diversos instrumentos internacionales garantizan y protegen los derechos de las personas para poder no solamente usar este tipo de tecnologías, sino también para el desarrollo y la protección de las mismas. En este sentido, se han pronunciado los instrumentos universales, tales como la Declaración Universal de Derechos Humanos ("DUDH") y el Pacto Internacional de Derechos Económicos, Sociales y Culturales ("PIDESC"), así como, a nivel interamericano, lo ha hecho el Protocolo Adicional a la Convención Americana Sobre Derechos Humanos en Materia de Derechos Económicos, Sociales y Culturales ("Protocolo De San Salvador").

Los instrumentos internacionales antes mencionados recogen y garantizan el derecho al trabajo como un derecho humano[10], lo que evidencia la uniformidad de criterios con relación a esta prerrogativa, a pesar de las particularidades de cada una de las disposiciones correspondientes. De esta forma, desde la redacción de la DUDH, los diferentes instrumentos han ido desarrollando y adaptando las definiciones a las particularidades específicas. Así, en el PIDESC se establece que el derecho al trabajo comprende el derecho de toda persona a tener la oportunidad de ganarse la vida, mediante un trabajo libremente escogido o aceptado y establece que los Estados deben adoptar diversas medidas para lograr la plena efectividad del derecho, entre las cuales incluye normas y técnicas encaminadas a conseguir un desarrollo económico, social y cultural constante y la ocupación plena y productiva.

El instrumento regional, el Pacto de San Salvador, establece que las personas tienen el derecho al trabajo, el cual incluye la oportunidad de obtener los medios

---

9 Constitución de la República del Ecuador. Publicada en el Registro Oficial el 20 de octubre del 2008. Artículos 11 numeral 3 y 417.

10 "Toda persona tiene derecho al trabajo, a la libre elección de su trabajo, a condiciones equitativas y satisfactorias de trabajo y a la protección contra el desempleo." Declaración Universal de Derechos Humanos (1948). Artículo 23. "1. Los Estados Partes en el presente Pacto reconocen el derecho a trabajar, que comprende el derecho de toda persona a tener la oportunidad de ganarse la vida mediante un trabajo libremente escogido o aceptado, y tomarán medidas adecuadas para garantizar este derecho". Pacto Internacional de Derechos Económicos, Sociales y Culturales (1968). Artículo 6. "1. Toda persona tiene derecho al trabajo, el cual incluye la oportunidad de obtener los medios para llevar una vida digna y decorosa a través del desempeño de una actividad lícita libremente escogida o aceptada". Protocolo Adicional a la Convención Americana Sobre Derechos Humanos en Materia de Derechos Económicos, Sociales Y Culturales (1988). Artículo 6.

para llevar una vida digna y decorosa, a través del desempeño de una actividad lícita, libremente escogida o aceptada y, adicionalmente, establece que los Estados se comprometen a adoptar las medidas que garanticen la plena efectividad del derecho al trabajo, en especial, las referidas al logro del pleno empleo.

Por lo tanto, es evidente que los Estados, a través de la adopción de los diferentes instrumentos internacionales, tanto universales como regionales, han reconocido el derecho al trabajo como un derecho fundamental, comprometiéndose a adoptar ciertas medidas para lograr la plena consecución de tal derecho.

En el análisis realizado es importante también incluir el derecho humano al acceso al internet, declarado así por la Asamblea General de las Naciones Unidas[11], el cual tiene un papel importante en el tema en cuestión. Sobre este asunto, el Relator Especial ha dicho que "Internet se ha convertido en un instrumento indispensable para ejercer diversos derechos humanos, luchar contra la desigualdad y acelerar el desarrollo y el progreso humanos, la meta del acceso universal a Internet ha de ser prioritaria para todos los Estados"[12], lo que evidencia el papel cada vez más interesante que el internet ha adquirido.

Por lo tanto, los derechos humanos, en cierta medida, ponen límites que los Estados no pueden sobrepasar al momento de regular tales innovaciones, entonces, estos deben observar, garantizar y respetar, en todo momento, el cumplimiento de las obligaciones internacionales. Por lo tanto, como los derechos humanos regulan los Estados, estos deben precautelar, en todo momento, los derechos de las personas, sobre todo, en cuanto al trabajo se refiere, por lo tanto, una regulación contraria a estos derechos es, a todas luces, inaceptable. A pesar de que los instrumentos internacionales limitan la actuación contraria a los derechos de las personas, la Constitución tiene disposiciones que obligan al Estado a tener, no solamente un mayor respeto, sino también a apoyar las nuevas tecnologías, lo que se analizará en la siguiente sección.

5. Derechos Constitucionales

Con el fin de desarrollar un análisis completo sobre esta materia, es importante tomar en cuenta el ordenamiento jurídico ecuatoriano y considerar, principalmente, los derechos reconocidos y garantizados en la norma jerárquicamente superior: la Constitución. Este cuerpo normativo recoge varios principios y derechos importantes en este asunto, los cuales serán analizados en la presente sección.

---

11 La Asamblea General de las Naciones Unidas aprobó el Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue. Promoción, protección y disfrute de los derechos humanos en Internet. Resolución A/HRC/20/L.13 de 29 de junio de 2012.

12 Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue. Promoción, protección y disfrute de los derechos humanos en Internet. Resolución A/HRC/20/L.13 de 29 de junio de 2012.

El primer derecho Constitucional que se analizará es el derecho al trabajo, el cual, al igual que los derechos humanos, también se encuentra garantizado ampliamente en nuestra normativa interna. De esta forma, la Constitución reconoce en el artículo 33 que "*el trabajo es un derecho y un deber social, y un derecho económico, fuente de realización personal y base de la economía"*[13]. Con la lectura del presente artículo se evidencia claramente que la Constitución reconoce, inequívocamente, que el trabajo es un derecho que configura la base de la economía y que el Estado tiene la obligación de garantizarlo. En este sentido, se encuentran las disposiciones del art. 325[14], en el cual se establece expresamente tal obligación estatal. Esta disposición es importante, puesto que menciona que se reconocen y garantizan todas las modalidades de trabajo, sean bajo relación de dependencia o no. La normativa va más allá, cuando establece que la política económica del Estado tiene como uno de sus objetivos principales la valoración de todas las formas de trabajo y el impulso del pleno empleo, este último, a su vez, es uno de los principios fundamentales del derecho al trabajo junto con la eliminación del desempleo[15].

En el mismo sentido, la Constitución, con relación a los derechos de libertad, establece también que el Estado reconoce y garantiza el derecho a la vida digna de las personas, derecho que incluye un trabajo o empleo, así como el derecho a desarrollar actividades económicas, en forma individual o colectiva, conforme a los principios de solidaridad, responsabilidad social y ambiental y también el derecho a la libertad de contratación. En la misma disposición también se incluye el derecho que tienen las personas a la libertad de trabajo[16]. Como se evidencia en los artículos antes mencionados, la Constitución garantiza en varias de sus disposiciones el derecho al trabajo, lo cual, en sintonía con los instrumentos internacionales de derechos humanos, protege y alienta a los ciudadanos y a las personas en general al uso y desarrollo de la tecnología en el trabajo.

Si bien el Estado garantiza ampliamente el derecho al trabajo, no es el único derecho ni principio relevante en el marco constitucional para el tema en cuestión. De esta forma, la Constitución también reconoce que las personas tienen derecho al acceso universal de las tecnologías de información y comunicación, así como a la

---

13 Constitución de la República del Ecuador. Publicada en el Registro Oficial el 20 de octubre del 2008. Art. 33.

14 El Artículo 325 establece que "El Estado garantizará el derecho al trabajo. Se reconocen todas las modalidades de trabajo, en relación de dependencia o autónomas, con inclusión de labores de autosustento y cuidado humano; y como actores sociales productivos, a todas las trabajadoras y trabajadores".
Constitución de la República del Ecuador. Publicada en el Registro Oficial 449 de 20 de octubre del 2008. Art. 325.

15 Constitución de la República del Ecuador. Publicada en el Registro Oficial 449 de 20 de octubre del 2008. Artículos 284 y 326.

16 Constitución de la República del Ecuador. Publicada en el Registro Oficial 449 de 20 de octubre del 2008. Artículo 66 numerales 2, 15, 16 y 17.

promoción por parte del Estado del acceso equitativo a los factores de producción, en donde el Estado debe impulsar y apoyar el desarrollo y la difusión de conocimientos y tecnologías orientados a los procesos de producción, así como evitar la concentración o el acaparamiento de factores y recursos productivos, promover su redistribución y eliminar privilegios o desigualdades en el acceso a ellos[1]. Como se ha visto, las tecnologías disruptivas producen y promueven justamente los procesos de producción, generando alternativas distintas a las existentes y, en concordancia con lo mencionado al inicio del presente capítulo, nuevas plazas y espacios de trabajo.

Las tecnologías disruptivas, por su naturaleza, cumplen con lo determinado en el artículo 52 de la norma jerárquicamente superior. El artículo al que se hace referencia establece que las personas tienen derecho a disponer de bienes y servicios de óptima calidad y a elegirlos con libertad, lo cual está íntimamente relacionado con el derecho a acceder a bienes y servicios públicos y privados de calidad, con eficiencia, eficacia y buen trato, así como a recibir información adecuada y veraz sobre su contenido y características, derecho que está garantizado en el artículo 66 de la Constitución. En cuanto a la regulación, esta norma también tiene disposiciones, las cuales establecen que el Estado tiene la obligación de evitar los monopolios y oligopolios privados, lo que se encuentra en concordancia con la Ley de Control y Poder del Mercado que prohíbe impedir o restringir el acceso de operadores económicos a la provisión de bienes y servicios.

Por último, debemos también tomar en cuenta uno de los pilares fundamentales de la Constitución y de los deberes fundamentales del Estado: el Buen Vivir o *Sumak Kawsay*[2]. Para la consecución de este principio, el Estado tiene ciertos deberes generales, entre los cuales se destaca la promoción y el impulso de la ciencia, tecnología y, en general, las actividades de la iniciativa creativa comunitaria, asociativa, cooperativa y privada, esto sumado al impulso del desarrollo de las actividades económicas, mediante un orden jurídico e instituciones políticas que las promuevan, fomenten y defiendan por medio del cumplimiento de la Constitución y la ley[3].

---

1 Constitución de la República del Ecuador. Publicada en el Registro Oficial 449 de 20 de octubre del 2008. Artículo 16 numeral 2 y Artículo 334 numerales 1 y 3.

2 Sumak Kawsay es la traducción literal de Buen Vivir a Kichwa, que de acuerdo a la Constitución es uno de los idiomas oficiales de la relación intercultural. Estos términos son utilizados indistintamente en la Carta Magna ecuatoriana. Este concepto no tiene definición exacta, sin embargo en el Plan Nacional del Buen Vivir se establece que este “es la forma de vida que permite la felicidad y la permanencia de la diversidad cultural y ambiental; es armonía, igualdad, equidad y solidaridad. No es buscar la opulencia ni el crecimiento económico infinito”.

3 Constitución de la República del Ecuador. Publicada en el Registro Oficial 449 de 20 de octubre del 2008. Artículos 277 numerales 5 y 6.

En la actualidad, este concepto tiene tal importancia en el país que existe un Plan Nacional del Buen Vivir, el cual es "la hoja de ruta de la actuación pública para construir los derechos de las personas"[4], en el cual se establece el uso de la tecnología en diversos sectores y el planteamiento de objetivos dentro de este lineamiento, lo cual evidencia y refuerza las obligaciones estatales con relación al asunto materia de este artículo.

Como se evidencia, las tecnologías disruptivas, por esencia, cumplen lo establecido en la Constitución, por lo cual, el Estado, en cumplimiento de las obligaciones contenidas en la Carta Magna, no solamente debería garantizar el uso y la creación de negocios con la utilización de la tecnología, sino que debería incentivarlos.

6. Conclusión

Claramente existe una mayor presencia de las tecnologías disruptivas en la actividad diaria del ciudadano. Aquellas evolucionan de manera progresiva y, en algunos casos, exponencial, junto con la evolución del conocimiento informático.

Aquel proceso de crecimiento y desarrollo de las tecnologías, sin duda, supera el desarrollo legislativo y regulatorio de los estados y de las administraciones públicas, requiriendo, por lo tanto, una mayor celeridad y adaptabilidad de las administraciones públicas ante tales procesos tecnológicos.

El asunto revierte particular importancia, pues podría suceder, como se observa ya en varios países, que tales administraciones públicas se quedasen en una situación tal que no puedan satisfacer los intereses de los ciudadanos por su ausencia de dinamismo e innovación en la regulación.

En el caso ecuatoriano, la Constitución impone al Estado un mandato de innovación y desarrollo tecnológico, mandato que implementarse para la oportuna adecuación del ordenamiento jurídico a las nuevas tecnologías.

4 Plan Nacional para el Buen Vivir 2013.2017. Publicado en el Registro Oficial Suplemento 78 de 11 de septiembre de 2013.

El impacto de la Ley Orgánica de Comunicación en la libertad de expresión en internet

Daniela Salazar Marín
Universidad San Francisco de Quito

RESUMEN: Si bien la Ley Orgánica de Comunicación de Ecuador señala que su ámbito de aplicación excluye el internet, en la práctica, la entrada en vigencia de esta Ley ha tenido un impacto perjudicial en la libertad de expresión en internet.

PALABRAS CLAVE**:** internet, Ley de Comunicación, derechos digitales, libertad de expresión, medios digitales, intermediarios de internet.

ABSTRACT: While the Ecuadorean Communications Law states that its scope of application excludes the Internet, in practice the issuance of this Law has had a detrimental impact on the freedom of expression through the Internet.

KEYWORDS: internet, Communications Law, digital rights, freedom of expression, digital media, internet intermediaries.

1. Introducción

La Ley Orgánica de Comunicación, en principio, no regula la información u opinión que de modo personal se emita a través de internet. Es claro que si sería posible aplicar el régimen sancionatorio de dicha Ley a los contenidos difundidos por medio de internet en Ecuador, estaríamos muy lejos de un internet libre de censura. No obstante, resulta ingenuo asumir que la vigencia de la Ley Orgánica de Comunicación no ha tenido un impacto en la libertad de expresión en la red.

Mediante este texto pretendo demostrar que la vigencia de la Ley Orgánica de Comunicación ha limitado la libertad de recibir, buscar y difundir ideas y opiniones por medio de internet en Ecuador. Con base en los más elementales estándares de derechos humanos relativos a internet, procuraré desvirtuar la idea de que la mencionada Ley excluye, por completo, al internet de su ámbito de aplicación. Para ello, me referiré, en primer lugar, a cómo la Ley Orgánica de Comunicación genera incentivos para que los medios de comunicación tradicionales se conviertan en censores privados de los comentarios que terceras personas publican a través de los portales de internet. Luego, explicaré cómo la Ley Orgánica de Comunicación omite proteger el derecho al anonimato en internet. El resultado de estas normas, aunque han pasado desapercibidas frente a otras preocupantes disposiciones de la misma Ley, ha sido nefasto para la vigencia de los derechos a la libertad de expresión y a la privacidad en internet en Ecuador.

2. La Ley Orgánica de Comunicación genera fuertes incentivos para que los medios se conviertan en censores privados

El ámbito de aplicación de la Ley Orgánica de Comunicación (en adelante, también “LOC”) está delimitado en sus primeros artículos. De ellos se desprende que la Ley regula, en el ámbito administrativo, los “contenidos comunicacionales”, a los que define como “todo tipo de información u opinión que se produzca, reciba, difunda e intercambie a través de los medios de comunicación social” (Artículo 3). Por medios de comunicación social, la LOC se refiere únicamente a los medios tradicionales de comunicación, es decir, “medios impresos o servicios de radio, televisión y audio y vídeo por suscripción” (Artículo 5). De hecho, este cuerpo legal, gracias a la acertada intervención de varios asambleístas[1], excluyó expresamente al internet de su ámbito de regulación, al señalar que la LOC “no regula la información u opinión que de modo personal se emita a través de Internet” (Artículo 4).

---

1 Los Asambleístas César Montúfar, Fausto Cobo y Jimmy Pinargote enviaron a la Comisión Especializada Comunicacional de la Asamblea Nacional, un memorando, con fecha 27 de Julio de 2011, advirtiendo cómo el artículo 5 del proyecto de Ley pretendía extender los efectos de la ley a “todo mensaje que se difunda por cualquier medio, formato o *plataforma tecnológica* [...]” (el resaltado me pertenece).

De la lectura de estos artículos podríamos inferir que la LOC no tiene impacto alguno en el internet en Ecuador, por lo que este ensayo resultaría innecesario. No obstante, la Ley de Comunicación advierte que los contenidos de los medios de comunicación "pueden ser generados o replicados por el medio de comunicación a través de Internet" (Artículo 5) y extiende su alcance a todos los contenidos publicados en internet por los medios tradicionales.

Pero, más allá de que las páginas de internet de los medios de comunicación se consideren, para efectos de la LOC, una extensión del medio de comunicación, lo que realmente me preocupa es la manera en que esta legislación impone a los medios tradicionales responsabilidades que fomentan la censura y, en consecuencia, resultan incompatibles con la libertad de expresión. Esto ocurre, como explicaré a continuación, cuando los medios de comunicación tienen portales de internet y actúan como intermediarios de internet. En sentido amplio, son intermediarios de internet todos aquellos agentes que facilitan o realizan transacciones para terceras partes en Internet (OECD: 2011, 21). Los proveedores de servicio de internet, los motores de búsqueda o las plataformas de redes sociales son todos intermediarios de internet y, como tales, desempeñan una función vital para que la gente de todo el mundo pueda comunicarse entre sí (ARTICLE 19, 2013). En este sentido, cuando los medios de comunicación actúan como proveedores de contenido en internet, así como cuando facilitan la interacción de terceras personas a través de sus portales de internet, están actuando como intermediarios de internet.

Así, el Artículo 20 de la LOC[2] establece un régimen de responsabilidad condicionada para los medios de comunicación, respecto de los comentarios que los usuarios formulen a través de las páginas de internet de tales medios, que en la práctica se equipara a un régimen de responsabilidad objetiva. Según esta norma, los comentarios de los usuarios son, en principio, de responsabilidad personal, excepto cuando los medios incumplen cualquiera de estas tres obligaciones: (i) la de informar de manera clara al usuario sobre su responsabilidad personal respecto de los comentarios emitidos; (ii) la de generar mecanismos de registro de los datos personales que permitan su identificación; o (iii) la de diseñar e implementar mecanismos de autorregulación que eviten la publicación y permitan la denuncia y eliminación de contenidos que lesionen los derechos consagrados en la Constitución y la ley.

2 Ley Orgánica de Comunicación Art. 20.- Responsabilidad ulterior de los medios de comunicación.- [...] Los comentarios formulados al pie de las publicaciones electrónicas en las páginas web de los medios de comunicación legalmente constituidos serán responsabilidad personal de quienes los efectúen, salvo que los medios omitan cumplir con una de las siguientes acciones: 1. Informar de manera clara al usuario sobre su responsabilidad personal respecto de los comentarios emitidos; 2. Generar mecanismos de registro de los datos personales que permitan su identificación, como nombre, dirección electrónica, cédula de ciudadanía o identidad, o; 3. Diseñar e implementar mecanismos de autorregulación que eviten la publicación, y permitan la denuncia y eliminación de contenidos que lesionen los derechos consagrados en la Constitución y la ley. [...]

Según el citado Artículo 20, el incumplimiento de una de estas obligaciones genera que el medio de comunicación asuma la responsabilidad por los comentarios que cualquier persona emita a través de su portal de internet, aun cuando no haya tenido participación en ellos. En consecuencia, resulta necesario detenernos en estas tres obligaciones para determinar si este régimen de responsabilidad condicionada impone obligaciones necesarias y proporcionales a los medios.

Respecto de la primera obligación: "informar de manera clara al usuario sobre su responsabilidad personal respecto de los comentarios emitidos", no cabe mayor análisis. No parece desproporcionado exigir que los medios de comunicación informen a quienes utilizan su plataforma para expresarse, que serán personalmente responsables por los contenidos que publiquen por su intermedio.

Respecto de la obligación de "generar mecanismos de registro de los datos personales que permitan su identificación", caben dos análisis. El análisis sobre cómo esta obligación incide en el derecho al anonimato, lo realizaré en la siguiente sección de este ensayo. Por ahora, me interesa mencionar que se trata de una obligación de cumplimiento imposible y, por lo tanto, desproporcionada. Si la ley se limitara a exigir un mecanismo de registro de datos que permita *contactar* a la persona que formuló el comentario, no habría problema. Sería cuestión de crear un usuario con un correo electrónico y luego enviar un correo a esa dirección para activar el usuario y así, confirmar que se trata de la misma persona. Pero exigir que los medios generen un mecanismo que permita *identificar* a quien formuló el comentario, demuestra un profundo desconocimiento de la arquitectura del internet.

Por ejemplo, hoy, yo podría registrar mis datos en el medio de comunicación y hacerme pasar por Taylor Swift, por Hilary Clinton o por Doña Chani, sin que el medio tenga posibilidad de identificar con certeza que detrás de esa cuenta está Daniela Salazar. Y, según la redacción de la Ley, basta que el mecanismo no permita identificar a quien formuló el comentario, para que toda la responsabilidad por los contenidos compartidos recaiga sobre el medio de comunicación, lo que, de hecho, les traslada la responsabilidad por contenidos de terceros, de manera absurda. Llama la atención que la Ley ni siquiera exija que exista un daño o un daño potencial, basta el incumplimiento de una obligación imposible, como la obligación de *identificar*, para transferir al medio la responsabilidad por los contenidos publicados por terceros.

Esta disposición se encuentra en franca contravención con lo recomendado por los Relatores sobre libertad de expresión en su Declaración Conjunta, cuando se refirieron al principio de mera transmisión y señalaron que

> "[n]inguna persona que ofrezca únicamente servicios técnicos de Internet como acceso, búsquedas o conservación de información en la memoria caché deberá ser responsable por contenidos generados por terceros y que se difundan a través de estos servicios, siempre que no intervenga específi-

camente en dichos contenidos ni se niegue a cumplir una orden judicial que exija su eliminación cuando esté en condiciones de hacerlo" (Declaración Conjunta, 2.a).

Finalmente, la más preocupante es la tercera obligación que exige a los medios diseñar e implementar mecanismos de autorregulación que eviten la publicación y permitan la denuncia y eliminación de contenidos que "lesionen derechos". Se trata, a todas luces, de un lenguaje demasiado amplio, vago y sujeto a distintas interpretaciones. Refiriéndose a legislaciones tan vagas, el actual Relator Especial de la ONU para la Libertad de Expresión ha señalado que

> "[s]uch language gives broad discretion to authorities to determine what kinds of digital expression would violate their terms. As a result, individuals and businesses are likely to err on the side of caution in order to avoid onerous penalties, filtering content of uncertain legal status and engaging in other modes of censorship and self-censorship" (Kaye: 2016, 39).

Como ha establecido la CIDH, citando el punto 2.b de la Declaración Conjunta sobre libertad de expresión e Internet de los Relatores sobre Libertad de Expresión,

> "[c]uando se trata de intermediarios de Internet, es conceptual y prácticamente imposible, sin desvirtuar toda la arquitectura de la red, sostener que los intermediarios tengan el deber legal de revisar todos los contenidos que circulan por su conducto o presumir razonablemente que, en todos los casos, está bajo su control evitar el daño potencial que un tercero pueda generar utilizando sus servicios. A este respecto, resulta claro que los intermediarios no deben estar sujetos a obligaciones de supervisión de los contenidos generados por los usuarios con el fin de detener y filtrar expresiones ilícitas" (CIDH: 2013, 96).

Una de las características que hacen maravilloso al internet es su capacidad de facilitar que miles de millones de personas, en todo el mundo, puedan expresar sus opiniones y acceder a las opiniones de otros, fomentando el pluralismo. No obstante, la obsesión por la censura previa que caracteriza a toda la Ley Orgánica de Comunicación impregnó también al internet, en tanto la Ley exige que los medios "eviten la publicación" de ciertos contenidos, convirtiéndolos en censores privados. Si un medio de comunicación en Ecuador no logra evitar que a través de su página web un tercer usuario publique un contenido que "lesione derechos", ese medio asume la responsabilidad por tal contenido. Evidentemente, la LOC contiene un fuerte incentivo para que los medios censuren incluso expresiones legítimas, ante la posibilidad de ser sancionados.

La CIDH ha advertido los peligros de una legislación tan insensata:

> "[r]esponsabilizar a un intermediario en el contexto de una red abierta, plural, universalmente accesible y expansiva, sería tanto como responsabi-

lizar a las compañías de teléfono por las amenazas que por vía telefónica una persona profiere a otra causándole con ello incertidumbre y dolor extremo" (CIDH: 2013, 97).

Ante la amenaza de una sanción legal respecto de un contenido que podría lesionar derechos sin que el medio de comunicación lo haya advertido, el medio lógicamente optará por impedir su circulación. De hecho, ante un régimen de responsabilidad condicionada tan absurdo, que se traduce en la práctica en un régimen de responsabilidad objetiva, la mayoría de medios de comunicación en Ecuador ha optado por no ofrecer el servicio a través del cual los terceros pueden expresar sus opiniones respecto de los contenidos publicados por el medio de comunicación en internet. Así, las consecuencias para el debate público y robusto de los contenidos que los medios publican a través de sus páginas web, han sido nefastas.

Aclaro aquí que no abogo por un régimen de inmunidad absoluta ni de sobre-protección de los medios de comunicación cuando actúan como intermediarios de internet. Un régimen de inmunidad absoluta podría favorecer la libertad de expresión, pero no impediría que se difundan expresiones no protegidas, como pornografía infantil o discursos de odio y podría incidir en la vigencia de otros derechos, como la privacidad o la honra. Me inclino por un régimen de inmunidad condicionada, pero, en mi opinión, las condiciones que ha establecido la LOC son desproporcionadas y desconocen el funcionamiento de internet.

Cuando la Ley Orgánica de Comunicación impuso a los medios la obligación de diseñar mecanismos que eviten la publicación y permitan la denuncia y eliminación de contenidos que lesionen derechos, les impuso un deber de monitoreo y vigilancia de los comentarios de terceras personas en internet bajo un criterio demasiado amplio. Tal obligación no solo desconoce que es posible que el medio de comunicación simplemente no tenga la capacidad operativa para revisar los contenidos publicados por terceras personas, sino que también desconoce que no necesariamente un medio de comunicación tenga la capacidad técnica para hacerlo.

Un medio que recibe cientos o miles de comentarios en un día, debería contratar a varios abogados con un entrenamiento técnico muy elevado para monitorear los comentarios y garantizar que no se publiquen contenidos que puedan lesionar derechos de terceros. La decisión de eliminar contenidos expresados por terceras personas a través de internet requeriría de un conocimiento jurídico muy elevado que permita identificar con claridad los casos de contenidos realmente antijurídicos o discriminatorios, capaces de producir daños o lesionar derechos que los medios están obligados a evitar. Además, antes de censurar comentarios, con el objetivo de salvaguardar el orden público, los medios tendrían que estar en la capacidad de "comprobar la existencia de causas reales y objetivamente verificables que planteen, cuando menos, una amenaza cierta y creíble de una perturbación potencialmente grave de las condiciones básicas para el funcionamiento de las ins-

tituciones democráticas" (CIDH: 2013, 62). Para que los medios puedan cumplir su deber respecto de expresiones no protegidas -como la propaganda de guerra y la apología del odio que constituya incitación a la violencia, la incitación directa y pública al genocidio, y la pornografía infantil-, deben someter su decisión a un juicio estricto de necesidad y proporcionalidad y garantizar que la censura no alcance a discursos legítimos que merecen protección, por más molestos que resulten. Además, "cualquier medida de este tipo debe ser adoptada solamente cuando sea la única medida disponible para alcanzar una finalidad imperativa y resultar estrictamente proporcionada al logro de dicha finalidad" (CIDH: 2013, 87).

Frente a tan estrictos estándares, ante la incertidumbre sobre una eventual responsabilidad respecto de contenidos controversiales o chocantes, resulta lógico que un medio de comunicación prefiera suprimir el comentario, antes que arriesgarse a una eventual responsabilidad. Y es que los medios de comunicación, reconozcámoslo, no necesariamente tienen un compromiso con la libertad de expresión de sus usuarios que supere sus intereses financieros. Aun cuando así fuera, no puede pretenderse que los medios de comunicación no maximicen su bienestar con el fin de reducir al máximo toda posibilidad de ser sancionados por publicar ciertos contenidos.

No hace falta ser un empresario de la comunicación para saber que será mucho más fácil para un medio de comunicación optar por suprimir la opción de comentarios de lectores a través de internet, antes que crear un mecanismo capaz de garantizar que no se publiquen comentarios que alguien pueda considerar contrarios a sus derechos, particularmente, conociendo la enorme sensibilidad que caracteriza a los funcionarios públicos en Ecuador. Como consecuencia de la entrada en vigencia de la LOC, los medios de comunicación en Ecuador optaron por suprimir la posibilidad de que los lectores expresen su opinión a través de sus portales digitales, lo que impidió que la Superintendencia se pronuncie, pero impidió también que ejerzamos nuestro derecho a transmitir nuestras ideas y opiniones por todos los medios que consideremos adecuados. Adicionalmente, se impidió que ejerzamos nuestro derecho a beneficiarnos de los comentarios y reacciones que leemos en internet y a interactuar, tanto con los autores de los contenidos publicados a través de las páginas de internet de los medios de comunicación, como con los otros lectores. El debate público y robusto, a través de internet, se ha visto enormemente perjudicado por la existencia de esta legislación.

A pesar de que tanto la Constitución como la propia LOC prohíben la censura previa, a las autoridades no parece haberles preocupado que la Ley incentive que los medios cierren este espacio de debate con el fin de evitar sanciones. Y respecto de los escasos medios que mantienen abierto ese espacio, no existen mecanismos de transparencia que nos permitan conocer qué tipo de comentarios se están censurando o cuestionar esas decisiones. No me cabe duda que el sistema instaurado ha provocado que los medios de comunicación, que aún mantienen espacios para

comentarios en línea por parte de sus lectores, remuevan contenidos legítimos, incluso especialmente protegidos. Pero el mensaje que envía la LOC es claro: no se sancionan los casos en que los medios censuren expresiones legítimas, sino solo los casos en que los medios no hayan logrado evitar ciertas publicaciones.

La decisión del Estado se explica, quizá, porque a las autoridades les resulta más fácil identificar y coaccionar a los medios en su calidad de intermediarios, que a los responsables directos de la expresión que se busca remover, tanto por la dificultad de identificarlos, como también por la posibilidad de que se encuentren en múltiples jurisdicciones. Además, como ha resaltado la CIDH, "existe un mayor incentivo económico en buscar la responsabilidad de un intermediario que en buscar la de un usuario individual" (CIDH: 2013, 93).

El Ex Relator de la ONU para la Libertad de Expresión advirtió que

> "[l]a responsabilización de los intermediarios con respecto al contenido difundido o creado por sus usuarios menoscaba gravemente el disfrute del derecho a la libertad de opinión y de expresión, pues da lugar a una censura privada de autoprotección excesivamente amplia, a menudo sin transparencia y sin las debidas garantías procesales" (La Rue: 2011, 40).

Por su parte, el actual Relator ha señalado que

> "[i]t is also critical that private entities ensure the greatest possible transparency in their policies, standards and actions that implicate the freedom of expression and other fundamental rights. Human rights assessments should be subject to transparent review, in terms of their methodologies, their interpretation of legal obligations and the weight that such assessments have on business decisions. Transparency is important across the board, including in the context of content regulation, and should include the reporting of government requests for takedowns" (Kaye: 2016, 89).

En contraposición a estas recomendaciones, la Ley Orgánica de Comunicación no exige que los medios respeten garantías de debido proceso antes de proceder con la censura de los comentarios o con su eliminación posterior a una denuncia. Para la LOC, la primera opción parece ser la censura, sin que se exija a los medios explicar los criterios para evitar la publicación de ciertos contenidos y comunicarse con la persona que está tratando de publicarlos. Luego, solo si los medios no evitan la publicación de tales contenidos, la LOC parece inclinarse por un sistema de notificación y retiro que ofrece a usuarios que consideren que un contenido es ilegal, la posibilidad de notificar al medio para que este inmediatamente dé de baja ese contenido, nuevamente sin necesidad de notificar a quien generó el contenido, lo que puede prestarse para abusos. Nótese que en ningún momento la Ley menciona la necesidad de que exista una intervención judicial, ni se inclina por un sistema en el que la responsabilidad se traslade a los medios únicamente cuando

se nieguen a cumplir una orden judicial, ni siquiera instauró un sistema de notificación y contranotificación.

La obligación impuesta a los medios de comunicación, respecto de las expresiones de terceras personas difundidas a través de sus portales de internet, es contraria también a los Principios de Manila sobre responsabilidad de intermediarios, adoptada en 2015 por un grupo de organizaciones de la sociedad civil. Tal como está establecida la atribución de responsabilidad a los medios en Ecuador, se incumple, al menos, con los siguientes principios: 1. Los intermediarios deben ser protegidos por ley de responsabilidad por el contenido de terceros; 2. No debe requerirse la restricción de contenidos sin una orden emitida por una autoridad judicial; 3. Las solicitudes de restricción de contenido deben ser claras, inequívocas, y respetar el debido proceso; y 4. Las leyes, órdenes y prácticas de restricción de contenidos deben cumplir con los *tests* de necesidad y proporcionalidad.

Dado que existen evidentes alternativas, menos gravosas para el derecho a la libertad de expresión, que podrían haberse aplicado para que los medios den de baja únicamente aquellos contenidos no protegidos por el derecho a la libertad de expresión, en el marco de un régimen transparente y respetuoso del debido proceso, es claro que la medida no cumple con el principio de necesidad. En cuanto a la falta de proporcionalidad, también resulta evidente que el beneficio de la medida ha sido mínimo en comparación con las afectaciones, tanto a nivel del afectado directo, como del conjunto de la sociedad, no solo considerando las posibles expresiones legítimas que no han sido publicadas por los medios, sino, sobre todo, considerando que la mayoría de medios optaron por remover la opción de comentarios de los usuarios, inhibiendo el debate público. Los medios se han visto obligados por la Ley a restringir expresiones, sin que la misma Ley les exija salvaguardas que eviten el abuso de este deber, tales como transparencia respecto de los contenidos cuya remoción haya sido ordenada, así como información pormenorizada sobre su necesidad y justificación.

En conclusión, cuando la Ley Orgánica de Comunicación exige a los medios, en su calidad de intermediarios de contenidos basados en los comentarios publicados en sus páginas de internet, que controlen el contenido generado por sus usuarios con el fin de evitar la publicación de expresiones que podrían "lesionar derechos", les impone una obligación tan difusa y desproporcionada que termina por convertirse en una responsabilidad objetiva. Es claro que la LOC favorece un sistema de censura previa (evitar la publicación), en vez de optar por uno que permita la libre circulación de ideas, aunque con garantías procesales básicas, como la de definir previamente las categorías de expresiones prohibidas o los criterios para impedir su circulación, la de informar o notificar a las partes afectadas sobre la decisión de censurar la opinión y la de otorgarles una posibilidad real de impugnar la decisión.

"[L]a exigencia de remover contenidos por parte de los intermediarios, como condición para no ser considerados responsables por una expresión ilícita, solamente debería proceder cuando sea ordenada por una autoridad judicial o de naturaleza similar, que opere con suficientes garantías de independencia, autonomía e imparcialidad y que tenga la capacidad para evaluar los derechos en juego y ofrecer las garantías necesarias al usuario" (CIDH: 2013, 106).

3. La Ley Orgánica de Comunicación no garantiza el derecho de expresarnos desde el anonimato a través de internet

A lo largo de la historia, la posibilidad de expresarse desde el anonimato, sea en plazas públicas o a través de folletos e incluso libros anónimos, ha sido esencial para que las personas puedan criticar a la tiranía, cuestionar leyes y prácticas opresivas o manifestar su opinión sin ser descalificados personalmente. La protección del discurso anónimo es igual de importante en Internet.

Son dos las disposiciones de la Ley Orgánica de Comunicación que, en mi opinión, no garantizan adecuadamente el derecho al anonimato en internet. La primera, mencionada en la sección anterior, se encuentra en el Artículo 20 y se refiere a la obligación que tienen los medios de comunicación de generar mecanismos de registro de datos personales que permitan *identificar* a los usuarios que comentan la información u opinión publicada a través del portal de internet del medio, bajo amenaza de asumir la responsabilidad por tales publicaciones si no fuera posible identificar al usuario que las emitió. La segunda, también en el Artículo 20, señala que los medios de comunicación solo podrán reproducir mensajes de las redes sociales "cuando el emisor de tales mensajes esté debidamente identificado", bajo amenaza de asumir "la misma responsabilidad establecida para los contenidos publicados en su página web que no se hallen atribuidos explícitamente a otra persona" si no cumplen con la obligación de identificarlos debidamente.

El derecho al anonimato está protegido por el derecho a la privacidad, como parte del derecho a no ser objeto de injerencias arbitrarias en nuestra vida. Se trata de un derecho estrechamente relacionado con la libertad de expresión, en tanto permite que un individuo pueda formarse libremente una opinión, expresar sus ideas y buscar o recibir información, "sin ser forzado a identificarse o a revelar sus creencias y convicciones o las fuentes que consulta" (CIDH: 2013, 132). Como ha señalado la CIDH, "[l]a protección del derecho a la vida privada implica al menos dos políticas concretas vinculadas al ejercicio del derecho a la libertad de pensamiento y expresión: la protección del discurso anónimo y la protección de los datos personales" (CIDH: 2013, 133).

A través de las citadas disposiciones de la LOC, el legislador olvidó por completo que la protección del discurso anónimo "favorece la participación de la personas en el debate público" (CIDH: 2013, 133). La posibilidad de crear cuentas anónimas en

redes sociales o para emitir comentarios a través de los portales de internet de los medios de comunicación permite, por ejemplo, que las personas se expresen sin temor a represalias personales, lo que puede ser especialmente relevante cuando se trata de personas que defienden posturas chocantes, minoritarias o contrarias frente a quienes ejercen posiciones de poder. Si los medios están obligados a adoptar medidas que les permitan identificar a los emisores de esos contenidos antes de permitir que esa información sea publicada en su portal de internet, o antes de citar esa opinión o información como fuente, se afecta el derecho de esas personas a opinar o informar libremente y, al mismo tiempo, por la doble dimensión del derecho a la libertad de expresión[3], necesariamente existe también una afectación al derecho de otros a recibir esas opiniones o informaciones.

Por supuesto que quienes emiten discursos no protegidos por el derecho a la libertad de expresión no pueden resguardarse en el anonimato de la responsabilidad generada por sus expresiones, pero esos casos podrían ventilarse a través de procesos judiciales que, en un marco de garantías y debido proceso, ordenen la adopción de medidas dirigidas a develar la identidad del emisor de mensajes no protegidos. Las garantías de expresión anónima no son absolutas, pueden ser limitadas, pero siempre en el marco de un procedimiento judicial que garantice una adecuada valoración de los derechos en juego. Dado que esa alternativa, menos gravosa para el derecho a la libertad de expresión, no resulta necesario ni proporcional adoptar medidas tan drásticas contra el anonimato como las de exigir que los medios puedan identificar a quienes formulan comentarios a través de sus portales de internet o a quienes difunden contenidos a través de redes sociales.

Nuevamente, resulta aplicable la analogía del teléfono. Yo puedo utilizar mi teléfono tanto para cometer un delito como para denunciar un delito, pero con el fin de evitar que se cometan delitos no sería proporcional prohibir los teléfonos públicos. No ignoro que a través de internet se pueden cometer delitos y que las nuevas tecnologías y el anonimato dificultan la investigación de estos delitos, pero eso no necesariamente justifica que se adopten medidas contrarias al anonimato. Por el contrario, el anonimato puede proporcionar protección a las personas para que no sean objeto de injerencias y ataques de actores estatales y no estatales y, por lo tanto, el Estado debería proteger y garantizar el anonimato.

Como ha sostenido el Relator Especial de la ONU para la Libertad de Expresión, se debe promover la existencia de espacios en línea libres de observación o docu-

---

3 Sobre la doble dimensión del derecho a la libertad de expresión, véase: Corte I.D.H., Caso Kimel Vs. Argentina. Fondo, Reparaciones y Costas. Sentencia de 2 de mayo de 2008. Serie C No. 177, párr. 53; Corte I.D.H., Caso Claude Reyes y otros. Sentencia de 19 de septiembre de 2006. Serie C No. 151, párr. 75; Corte I.D.H., Caso Herrera Ulloa. Sentencia del 2 de julio de 2004, Serie C No. 107, párr. 108; Corte I.D.H., Caso Ivcher Bronstein Vs. Perú. Sentencia de 6 de febrero de 2001. Serie C No. 74, párr. 146; Corte I.D.H., La Colegiación Obligatoria de Periodistas (arts. 13 y 29 Convención Americana sobre Derechos Humanos). Opinión Consultiva OC-5/85 del 13 de noviembre de 1985. Serie A No. 5, párr. 30.

mentación de la actividad e identidad de los ciudadanos. Esto incluye, en opinión del Ex Relator, la preservación de plataformas anónimas para el intercambio de contenidos y el uso de servicios de autenticación proporcionales (La Rue: 2013, 47).

Al evaluar la proporcionalidad de una medida, como la obligación de generar mecanismos de registro de datos personales que permitan *identificar* a los autores, debemos tener en cuenta no solo la afectación directa al particular, sino también el impacto de tal medida en el funcionamiento de la red. Desde el punto de vista de la persona afectada, la medida podría constituir una afectación leve, pero desde el punto de vista del derecho a la libertad de expresión de todo el conjunto de usuarios de medios de comunicación digitales, así como de redes sociales, este tipo de medidas han tenido un impacto devastador. Resulta difícil mensurar la cantidad de opiniones e informaciones que no se han emitido o difundido a causa de estas medidas.

Y es que algunas personas, al no tener garantizado su anonimato, por temor a represalias, prefieren no compartir opiniones e informaciones a través de los portales de internet de los medios de comunicación o a través de las redes sociales. La mayoría de medios, como ya apunté, optaron por suprimir la opción que tenían los usuarios de ingresar comentarios. Y, adicionalmente, los medios no pueden –sin hacerse personalmente responsables por esos contenidos- utilizar en sus notas de prensa opiniones e informaciones difundidas a través de redes sociales por personas que no puedan identificar, lo que solo es posible en casos excepcionales, como por ejemplo en Twitter, a través de la opción de cuentas verificadas. La exclusión de todas esas informaciones y opiniones del debate público que fomentan los medios de comunicación, nos perjudica a todos.

Las redes sociales pueden ser una fuente inagotable y valiosísima de informaciones y opiniones que los legisladores ecuatorianos prefirieron excluir de la discusión en los medios de comunicación tradicionales, sin que exista para ello un objetivo legítimo o imperioso. De hecho, si se toma en cuenta el supuesto fin de la Ley Orgánica de Comunicación que es la democratización de la información, resulta bastante contradictorio que se establezcan medidas legales que tiendan a excluir del debate público a las redes sociales, en tanto esas redes permiten ampliar las voces de quienes normalmente no tienen un espacio en los medios, así como también permiten multiplicar la información a la que tenemos alcance, exigiendo, de esta manera, que los medios se refieran a temas que quizá, sin la presión de redes sociales, no habrían sido cubiertos. Sinceramente, me cuesta comprender cuál es el interés que se busca proteger a través de la disposición que exige a los medios poder identificar adecuadamente a las personas que emiten informaciones y opiniones en redes sociales antes de poder divulgarlas. En consecuencia, me es imposible determinar si se trata de una medida necesaria, proporcional o conducente a tal fin.

El actual Relator Especial para la Libertad de Expresión, David Kaye, ha observado con particular preocupación las disposiciones de la Ley Orgánica de Comunicación en Ecuador (Kaye: 2015, 54) y ha sido enfático al señalar que los Estados no deben restringir el anonimato, en tanto facilita y, a menudo, contribuye al ejercicio del derecho a la libertad de opinión y de expresión. Incluso, en opinión del Relator, "los Estados deben abstenerse de establecer la identificación de los usuarios como condición para acceder a las comunicaciones digitales y a los servicios en línea" (Kaye: 2015, 60).

El Relator también ha hecho un llamado a que los Estados "velen porque los usuarios en peligro dispongan de las herramientas para ejercer su derecho a la libertad de opinión y de expresión de forma segura" (Kaye: 2015, 63). Ecuador ha hecho todo lo contrario. Exigir que los medios generen mecanismos de identificación de los usuarios para permitirles formular comentarios a través de sus portales de internet, sin que existan mecanismos adecuados para impedir la retención masiva de datos particulares o su mal uso, tiene también un impacto inhibidor en el debate. No podemos ignorar que mientras más permitamos que el Estado o los intermediarios recopilen y almacenen nuestros datos personales, mayor será la capacidad del Estado para llevar a cabo labores de vigilancia, así como mayor será el riesgo de que se robe y difunda nuestra información personal. Quienes sentimos la necesidad de resguardar nuestra seguridad y privacidad en línea, con el fin de buscar, recibir y difundir informaciones y opiniones sin riesgo de repercusiones, divulgación, vigilancia y otros usos indebidos de nuestra información privada, pensaremos dos veces antes de registrar nuestra información de contacto en la plataforma de un medio de comunicación, particularmente, si se trata de un medio público.

4. El internet no está libre de los efectos de la Ley Orgánica de Comunicación

Existen otras disposiciones de la LOC que, si bien no inciden directamente en los derechos digitales, extienden los efectos nocivos de la Ley al internet, por lo que las mencionaré brevemente. Por ejemplo, en casos en los que un medio de comunicación no dé paso, por su propia iniciativa, al derecho a la rectificación de una persona, la Superintendencia puede ordenar que el medio publique una rectificación y una disculpa pública "en su página web y en la primera interfaz de la página web del medio de comunicación por un plazo no menor a siete días consecutivos" (Artículo 23); en los casos de difusión de contenidos discriminatorios, la Superintendencia también puede ordenar que la disculpa pública de quien dirige el medio de comunicación se publique "en su página web y en la primera interfaz de la página web del medio de comunicación por un plazo no menor a siete días consecutivos" (Artículo 64); en casos en los que la Superintendencia determine que un medio difundió cifras falsas o inexactas de circulación de ejemplares, la Superintendencia puede ordenar

> "que el medio publique en la primera interfaz de su página web […] por el plazo de uno a siete días consecutivos, el reconocimiento de que las cifras de su tiraje no corresponden a la realidad, así como la correspondiente disculpa pública dirigida a las empresas, entidades y personas que pautaron publicidad o propaganda en dicho medio" (Artículo 90).

Así, el abuso del derecho de rectificación y réplica por parte del Estado, o la posibilidad de ahogar financieramente a los medios mediante multas relacionadas con obligaciones como la de dar publicidad al tiraje, ha impactado también el internet, a través de las páginas digitales de los medios de comunicación tradicionales.

A pesar de que el ámbito de regulación de la LOC excluye el internet, la sola vigencia de esta Ley ha tenido efectos respecto de la libertad de expresión en internet que merecen ser estudiados. Por ejemplo, la Ley Orgánica de Comunicación ha tenido como consecuencia la creación y el crecimiento exponencial de medios de comunicación digitales en Ecuador[4], lo que merece ser estudiado. Hoy en día, para evitar las sanciones de la LOC, gran parte del debate público plural y democrático ocurre a través de medios de comunicación digitales o en las redes sociales, a pesar de que solo un limitado grupo de personas tienen acceso a internet, en comparación con las personas que acceden a los medios tradicionales como la radio, la televisión o el periódico. Cabe preguntarse si con esto se ha avanzado, o no, hacia la democratización de la comunicación que la LOC supuestamente persigue.

Finalmente, si bien hasta ahora la Superintendencia de la Comunicación e Información no ha extendido su ámbito de acción al internet, no debemos ignorar que el Artículo 4 de la LOC excluye del ámbito de aplicación de la Ley únicamente la información u opinión que "de modo personal" se emita a través de internet. Es decir, no excluye la posibilidad de que la Superintendencia interprete que la información u opinión que de modo institucional – a través del portal de internet de un medio de comunicación- se emita a través de internet, se encuentra regulada también por la Ley Orgánica de Comunicación.

Lo anterior se confirma con la lectura del Artículo 3 del Reglamento General a la Ley Orgánica de Comunicación, según el cual

> "[s]on también medios de comunicación aquellos que operen sobre la plataforma de internet, cuya personería jurídica ha sido obtenida en Ecuador y que distribuyan contenidos informativos y de opinión, los cuales tienen los mismos derechos y obligaciones que la Ley Orgánica de Comunicación establece para los medios de comunicación social definidos en el Art. 5 de dicha Ley".

---

4 A marzo de 2013 existían 34 medios de comunicación nativos digitales, según un estudio de José Rivera Costales. El 25 de junio de 2013 se expidió la Ley Orgánica de Comunicación. Dos años después, en abril de 2015, la Organización Fundamedios había mapeado 60 medios nativos digitales.

Esto quiere decir que la información y opinión que se emite a través de los nuevos medios digitales que se han creado en Ecuador, se encuentran también regulados por la LOC, sea porque se emiten de manera institucional y no personal, como establece la Ley, o porque el Reglamento no se limitó a regular lo establecido en la LOC, sino que optó por ampliar el ámbito de aplicación de la Ley a los medios "que operen sobre la plataforma de internet" siempre que tengan personería jurídica en Ecuador. Si bien resulta discutible que un Reglamento pueda ampliar el ámbito de aplicación de una Ley, lo cierto es que las disposiciones de la LOC resultan aplicables también a los medios digitales que se han constituido en Ecuador.

5. Conclusiones

No existe un marco regulatorio adecuado para garantizar la libertad de expresión a través de internet en Ecuador. Nuestro país tiene pendiente ofrecer una adecuada tutela al derecho a la libertad de expresión, con miras a proteger adecuadamente la búsqueda, recepción y difusión de información e ideas de toda índole a través del internet. No es mi intención afirmar que la Ley Orgánica de Comunicación debió incluir al internet en su marco de acción, pero tampoco creo que es conveniente la ausencia de regulación y, lo que es peor, esta aparente no regulación que en la práctica termina por restringir ilegítimamente nuestra libertad de difundir y recibir informaciones e ideas por medio de internet.

Quizá hubiese sido mejor, en vez de una aparente no regulación, haber incluido en la legislación el principio de inviolabilidad de la libertad de difundir opiniones, información e ideas a través de medios digitales, acompañado de mecanismos claros de amparo frente a cualquier intervención arbitraria en esta libertad, así como en la libertad de comunicarnos de manera privada y anónima. En vez de pretender que el internet es un ámbito en el cual el Estado no interfiere, hubiese sido adecuado adaptar nuestra legislación a los principios internacionales en materia de derechos humanos aplicables al ejercicio de los derechos en internet reconociendo, como ha resuelto el Consejo de Derechos Humanos de la ONU, que "los mismos derechos que las personas tienen offline deben ser protegidos online, en particular el derecho a la libertad de expresión" (Consejo: 2016, 1).

Es necesario un cuerpo legal que regule adecuadamente la difusión de contenidos en el internet y que tenga en cuenta las características particulares de los medios digitales frente a los medios tradicionales. Como señalaron conjuntamente los Relatores sobre libertad de expresión: "[l]os enfoques de reglamentación desarrollados para otros medios de comunicación —como telefonía o radio y televisión— no pueden transferirse sin más a Internet, sino que deben ser diseñados específicamente para este medio, atendiendo a sus particularidades" (Declaración Conjunta: 2011, 1.c.).

En tanto internet se ha convertido en el medio más importante y dinámico para expresarnos y comunicarnos, resulta imprescindible que como usuarios de internet gocemos de garantías de libre circulación de información y opinión, sin que el gobierno ni los medios de comunicación, actuando como intermediarios, puedan censurar nuestras comunicaciones a través de internet. Esto incluye nuestro derecho a expresarnos desde el anonimato.

La LOC ha convertido a los medios de comunicación tradicionales en custodios de las expresiones vertidas en internet, así como de nuestros datos de identificación. No existen salvaguardas para garantizar que su rol de guardianes sea positivo para el libre mercado de ideas y se respeten los valores de libertad de expresión necesarios para facilitar el debate público robusto que un gobierno democrático supone.

Las exigencias que la Ley impone a los medios, bajo amenaza de asumir la responsabilidad por la información y opinión de terceros que se difunda por su intermedio, constituyen restricciones innecesarias y desproporcionadas que desnaturalizan el funcionamiento de internet y limitan su potencial democratizador como medio que está al alcance de un universo creciente de personas. Tales exigencias revelan un profundo desconocimiento de parte de los legisladores ecuatorianos sobre la manera cómo funciona internet, lo que, sumado al afán por la censura, ha tenido efectos perjudiciales en el debate público en Ecuador.

La Ley Orgánica de Comunicación, aunque afirme que excluye el internet de su ámbito de aplicación, ha tenido un impacto amplio y nocivo en nuestra capacidad de ejercer libremente nuestros derechos a la intimidad y a la libertad de opinión y de expresión en internet.

Bibliografía:

Article 19, *Internet Intermediaries: Dilemma of Liability*, Article 19, London, 2013.

Declaración conjunta sobre libertad de expresión e Internet. Relator Especial de las Naciones Unidas (ONU) sobre la Promoción y Protección del derecho a la Libertad de Opinión y de Expresión, Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), Relatora Especial de la Organización de Estados Americanos (OEA) para la Libertad de Expresión, y Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP). 1 de junio de 2011.

Comisión Interamericana de Derechos Humanos (CIDH). Relatoría Especial para la Libertad de Expresión. *Libertad de Expresión e Internet.* OEA/Ser.L/V/II. CIDH/RELE/INF. 11/13. 31 diciembre de 2013.

Corte I.D.H., *Caso Kimel Vs. Argentina*. Fondo, Reparaciones y Costas. Sentencia de 2

de mayo de 2008. Serie C No. 177.

Corte I.D.H., *Caso Claude Reyes y otros vs. Chile*. Sentencia de 19 de septiembre de 2006. Serie C No. 151.

Corte I.D.H., *Caso Herrera Ulloa vs. Costa Rica*. Sentencia del 2 de julio de 2004, Serie C No. 107.

Corte I.D.H., *Caso Ivcher Bronstein Vs. Perú*. Sentencia de 6 de febrero de 2001. Serie C No. 74.

Corte I.D.H., *La Colegiación Obligatoria de Periodistas (arts. 13 y 29 Convención Americana sobre Derechos Humanos)*. Opinión Consultiva OC-5/85 del 13 de noviembre de 1985. Serie A No. 5.

Cortés Castillo, Carlos. "Las llaves del ama de llaves: la estrategia de los intermediarios en Internet y el impacto en el entorno digital". En: *Internet y derechos humanos: aportes para la discusión en América Latina.* Bertoni, Eduardo (comp.) Buenos Aires: Del Puerto, 2014.

Fundamedios. *Listado de medios nativos digitales en Ecuador*. Abril de 2015.

Ley Orgánica de Comunicación (Ecuador). Registro Oficial No 22, publicado el 25 de junio de 2013.

Millaleo Hernández, Salvador, *Los intermediarios de Internet como agentes normativos. Revista de Derecho (Valdivia), vol. XXVIII, núm. 1, junio, 2015, pp. 33-54. Universidad Austral de Chile.* Valdivia, Chile.

Organización de las Naciones Unidas. Consejo de Derechos Humanos. *The promotion, protection and enjoyment of human rights on the Internet*. A/HRC/32/L.20, 27 de junio de 2016.

Organización de las Naciones Unidas. *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue*. A/HRC/23/40. 17 de abril de 2013.

Organización de las Naciones Unidas. Informe del Relator Especial de la ONU sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La *Rue*. A/HRC/17/27. 16 de mayo de 2011.

Organización de las Naciones Unidas. *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, David Kaye*. A/HRC/29/32. 22 de mayo de 2015.

Organización de las Naciones Unidas. *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, David Kaye*. A/HRC/32/38. 11 de mayo de 2016.

Organization for Economic Co-operation and Development OECD, *The Role of Internet Intermediaries in Advancing Public Policy Objectives.* OECD Publishing, Paris, 2011.

Reglamento General a la Ley Orgánica de Comunicación (Ecuador). Decreto Ejecutivo 214. Registro Oficial Suplemento 170 de 27 de enero de 2014.

Rivera Costales, José. "Medios digitales en Ecuador, cuántos son y qué hacen". *Revista Chasqui* No. 122, CIESPAL, junio de 2013.

Principios De Manila Sobre Responsabilidad De Los Intermediarios. Guía de Buenas Prácticas que Delimitan la Responsabilidad de los Intermediarios de Contenidos en la Promoción de la Libertad de Expresión e Innovación. 24 de Marzo de 2015.

Seng, Daniel. *Comparative Analysis of the National Approaches to the Liability of Internet Intermediaries*. WIPO, Ginebra, 2010.

Internet, niñez y adolescencia en Ecuador: una mirada general al estado de la cuestión

Farith Simon C.
Universidad San Francisco de Quito

RESUMEN: Si bien el internet puede ser una fuente de información, educación y de uso recreativo para niños, niñas y adolescentes, también puede ser un espacio de vulneración de sus derechos, razón por la que una revisión de la normativa es fundamental para el diseño de políticas públicas efectivas. Este análisis se plantea desde una perspectiva de derechos que abarca la legislación nacional e internacional aplicable.

PALABRAS CLAVE: Derechos de niños, niñas y adolescentes; nativos digitales; pornografía infantil; infancia y adolescencia.

ABSTRACT: While the Internet can be a source of information, education and recreational use for children and youth, it can also be a space for the violation of their rights, for this reason a revision of the norms and laws is important to consider for the design of effective public policies. This analysis is presented through a rights perspective that covers the applicability national and international legislation.

KEYWORDS: Rights of children and adolescents; digital natives; child pornography; childhood and adolescence.

1. Introducción

Los niños, niñas y adolescentes (NNA) están en el internet de muchas formas: como receptores pasivos de información, como activos usuarios que procesan y comparten contenidos, como creadores de contenidos, difundiendo sus opiniones, compartiendo material de su interés (Livingstone, S., y Haddon, 2009, p. 10) y de forma indirecta, por la utilización que los adultos hacen de sus datos e imágenes (Fernández, 2015, p. 35). El internet y, en general, las tecnologías de información y comunicación (TIC), ocupan un espacio tan relevante en la vida de NNA que son un elemento central en la cultura de las nuevas generaciones (Internet Society, s/f, y s/n).

Niños, niñas y adolescentes nacieron en la "Sociedad de la Información", son *nativos digitales*; un estudio del Observatorio para la Seguridad de la Información, de marzo de 2009, da cuenta de una sustancial diferencia entre el uso adulto y el de los niños, niñas y adolescentes; mientras los primeros usan el internet con una finalidad, es decir –de acuerdo al estudio citado, estudio- es "para algo"; niños, niñas y adolescentes reportan un uso más natural, es decir, "están" en internet para estudiar, para charlar o para escuchar música, etc., el internet es básico en sus relaciones sociales y en la construcción de identidad (Simon, 2011, p. 27).

Las oportunidades y los riesgos que existen en internet son múltiples, en el estudio más relevante que existe sobre el tema, Livingstone y Haddon (2009, p. 16) proponen una clasificación de estos cuando NNA se encuentran en línea, basada en tres posibles formas de comunicación: como receptor de muchas fuentes de información, en una interacción con adultos y comunicación con sus iguales, en esta él es el actor de la comunicación o el que la inició.

En la Web 2.0, los NNA como productores y consumidores de información dependen únicamente de su capacidad personal para acceder y producir información en Snapchat, Twitter, Facebook, Instagram, etc.; si bien, la mayoría de estas redes limitan el acceso a menores de ciertas edades, estos tienen una amplia presencia[1] desde corta edad, es muy difícil controlar el acceso a un medio en el que, con facilidad, se puede enmascarar la identidad.

Con las nuevas tecnologías de la comunicación e información los derechos de la infancia y adolescencia se han puesto a prueba en dos de sus condiciones esenciales, establecidas en la Convención sobre los Derechos del Niño[2]: el derecho a

1Facebook permite su uso a partir de los 14 años https://es-es.facebook.com/legal/terms/update?_fb_noscript=1; Twitter limita el acceso a mayores de 13 años http://www.twitterenespanol.net/privacy_policy.php; Snapchat restringe el uso a menores de 13 años http://www.twitterenespanol.net/privacy_policy.php; Instagram permite el uso a los mayores de 13 años https://www.instagram.com/about/legal/privacy/.

2 La Convención de los Derechos del Niño fue aprobada por unanimidad el 20 de noviembre de 1989,

la protección especial por la vulnerabilidad propia de su etapa de desarrollo y la condición de ser sujeto pleno de todos los derechos, lo que implica la posibilidad de ejercicio -progresivo- de esos derechos de manera directa. Protección especial y ejercicio progresivo entran en permanente tensión, en ocasiones estas se presentan como incompatibles o se da primacía a una de ellas. De la prioridad que se asigne a la tutela o al ejercicio progresivo de los derechos dependerán las respuestas que se otorguen normativamente. En último caso, la forma en la que se regule el uso del internet, con relación a la infancia, dependerá de cómo la percibimos.

En los últimos años se ha multiplicado el interés y la preocupación por este tema y, con ello, los debates y estudios. Entre los más relevantes: el Comité de los Derechos del Niño (CRC), el principal órgano de seguimiento de la CDN que organizó, en el año 2014, un "Día de debate General" acerca de "Medios digitales y derechos de la infancia[3]" ; Unicef publicó en 2014 el informe "Children's Rights in the Digital Age[4]"; CEPAL y UNICEF publicaron el estudio "Los derechos de la infancia en la era de Internet: América Latina y las nuevas tecnologías: América Latina y las nuevas tecnologías[5]"; en el marco de la Unión Europea, el estudio "EU Kids Online: Final report, 2009[6]" es especialmente relevante, además de la aprobación, por parte de la Comisión Europea, de los "Principios para redes sociales más seguras de la Unión Europea".

En Ecuador se cuentan con algunos datos que permiten entender el impacto que internet tiene en los menores de edad. En el año 2014, el 46,4% de la población usó internet (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2015, sin fecha); entre las personas jóvenes el porcentaje de uso es muy significativo: en aquellas que tienen entre 5 y 15 años, los usuarios ascendían a un 54,8%, en tanto que, en las personas que tienen entre los 16 y 24 años el porcentaje es del 67,8%. Un 83% de las personas que se conectan lo hicieron por medio de teléfonos inteligentes, el 17% restante a través de computadoras o tabletas. De acuerdo al Informe «Niñez y Adolescencia desde la Intergeneracionalidad» un 45% de los adolescentes ecuatorianos (de 12 a 18 años) están conectados a internet (Observatorio Social del Ecuador, 2016, p. 113). Existen 17'541.754 abonados a la telefonía móvil, este dato marca una diferencia en el acceso a internet en países desarrollados y en los que se encuentran en vías de desarrollo; en los primeros se da un

entró en vigor el 2 de marzo de 1990.

3 Committee on the Rights of the Child, Report of the 2014 Day of General Discussion "Digital media and children's rights", disponible en línea
http://www.ohchr.org/Documents/HRBodies/CRC/Discussions/2014/DGD_report.pdf

4 Third, A. et. al, Children's Rights in the Digital Age: A download from children around the world, Second edition, Young and Well Cooperative Research Centre, Melbourne, 2014.

5 Pavez, M. I., Los derechos de la infancia en la era de Internet: América Latina y las nuevas tecnologías, Cepal-Unicef, Cepal, Serie Políticas Sociales No. 210, Santiago, 2014.

6 Ob. Cit.

mayor ingreso por dispositivos móviles, en los segundos, por medio de conexiones fijas (Gasser, Urs, *et all,* 2010, p. 30*)*. En el mismo estudio se reporta que los sitios más visitados son Facebook y WhatsApp; los usuarios de Facebook ascendían en el año 2105 a 6'316.555. En el año 2015 el 20% de niños, niñas y adolescentes entre 8 y 17 años reportaron que ocupan su tiempo libre en navegar por internet; la primera actividad es la deportiva con un 73%; seguida de ver televisión con un 56% (Observatorio Social del Ecuador, 2016, p. 155).

Tabla 1: Clasificación de las oportunidades y los riesgos en línea para los niños*

		Contenido:	**Contacto:**	**Conducta:**
		Niño como destinatario	**Niño como participante**	**Niño como el actor**
Oportunidades	**Educación, aprendizaje y alfabetización digital.**	Recursos educativos	Contacto con otras personas que comparten intereses de uno	Iniciativa propia o colaborativa de aprendizaje
	Participación y compromiso cívico	Información global	Intercambio entre los grupos de interés,	Formas concretas de participación ciudadana
	Creatividad y la autoexpresión	La diversidad de los recursos	Ser invitado o inspirado para crear o participar	Creación de contenido generado por el usuario
	Identidad y conexión social	Asesoramiento (personal / salud / sexual, etc.)	Redes sociales, experiencias compartidas con los demás	Expresión de identidad
Riesgos	**Comercial**	Publicidad, correo no deseado, auspiciado	Seguimiento / recolección de información personal	Juegos de azar, descargas ilegales, piratería
	Agresivo	Contenido violento / grotesco / de odio	Ser acosado, hostigado o acechado	Intimidar o acosar a otra persona
	Sexual	Pornografía/ contenido sexual que hace daño	Conocer extraños, ser preparado (entrenado)	Creación y carga de material pornográfico
	Valores	Valores racistas, información o consejos sesgados (por ejemplo, drogas)	Daño auto infringido, persuasión no deseada	Brindar asesoramiento. Por ejemplo, en suicidios / anorexia

* Autoría: Livingstone, S., y Haddon, L., EU Kids Online: Final report, 2009, London School Of Economics and Political Science, 2009, LSE, London: EU Kids Online. Traducción al castellano: Hugo Cahueñas Muñoz.

Los datos disponibles dan cuenta de un crecimiento muy importante en el acceso a internet en los hogares: en el año 2010, el 12,3% de los hogares tenían acceso; en el 2013, el porcentaje se incrementó al 28,5%; en tanto que en el año 2015, el porcentaje llegó a un 31,4. En el año 2015 en el acceso a internet en los planteles educativos privados estaba en un 60%, en tanto que en los públicos llegaba a un 40% (Observatorio Social del Ecuador, 2016, p. 55).

No existen datos confiables actualizados en el país sobre las amenazas que enfrentan los NNA en las TIC's, en el informe «Niñez y Adolescencia desde la Intergeneracionalidad» al analizar el acoso escolar o *bullying* que tiene una alta incidencia en el país, se afirma que este se ha agudizado por las TIC's, exponiéndolos aún más a daños por acoso, más allá de las instituciones escolares[7].

El estudio más completo sobre el tema es "La Generación Interactiva en Iberoamérica 2010" (Bringué, Sabada y Tolosa, 2011[8]), en este se analiza los principales aspectos de la relación niñez y adolescencia e internet, pese a que su información data de 6 años atrás permite formarse una idea del uso que los ecuatorianos menores de edad dan a internet: la mayoría navega solo, con un 58,5% de prome-

7 En este sentido es equivocada la afirmación que realiza Luis Gustavo Guallpa Zatán que sostiene que el informe del Observatorio de la Niñez y Adolescencia el "Ecuador está ubicado en el segundo puesto como país Latinoamericano con más maltrato escolar; el 53% se realiza a través del Internet…" según una supuesta encuesta aplicada en el 2011. Este dato publicado en dos trabajos del autor con diferentes títulos, con parecido contenido ("Vulneración de derechos de niñ@s y adolescentes por el uso patológico de redes sociales digitales" presentado en el III Congreso Científico Internacional Uniandes: Impacto de las investigaciones universitarias, de 30 de julio de 2015, disponible en http://www.uniandes.edu.ec/web/wp-content/uploads/2016/04/Vulneración-de-derechos-de-niñ@s-y-adolescentes-por-el-uso-patológico-.pdf; "Redes sociales digitales y derechos de la niñez y adolescencia en Ecuador, publicado en Episteme, Revista de Ciencia y Tecnología e Innovación, Volumen 1, número 2 (2014), disponible en http://186.46.158.26/ojs/index.php/EPISTEME/article/view/32), sin embargo en los dos informes del ODNA publicados, el uno en el 2011 disponible en http://www.unicef.org/ecuador/Edna2011_web_Parte1.pdf, el otro en el 2016, disponible en http://www.unicef.org/ecuador/Ninez_Adolescencia_Intergeneracionalidad_Ecuador_2016_WEB2.pdf, se refiere a la violencia escolar y no entrega dato alguno sobre la violencia en redes. Un interesante trabajo "Protección a niños, jóvenes adolescentes y jóvenes adultos en internet, medios electrónicos y redes sociales" referido al Ecuador fue publicado en el portal del Observatorio Iberoamericano de Protección de Datos, trabajo de Héctor Revelo Herrera y Marco Trujillo, con datos al 2010 hace un recuento de la información disponible en ese año y una encuesta a 28 estudiantes de derecho informático y especialistas en seguridades informáticas sobre la percepción del "Cibercrimen y de los Derechos de los niños, jóvenes adolescentes y jóvenes adultos": ser persuadidos para que den información personal y familiar 67%, robo de identidad y datos personales 56%, ser persuadidos por alguien para conocerlo en persona 56%, alejamiento de sus relaciones en el mundo exterior por la constante interacción en una red social 48%, burlas – humillaciones entre compañeros de colegio a través de mensajes y publicación de contenidos 26%, discriminación debido a que un niño o joven no esté inscrito en una red social 15%, otros 48%. Este artículo se encuentra disponible en http://oiprodat.com/2014/05/01/proteccion-a-ninos-jovenes-adolescentes-y-jovenes-adultos-en-internet-medios-electronicos-y-redes-sociales/ .

8 Bringué, Sábada y Tolsá, "La Generación Interactiva en Iberoamérica 2010. Niños y adolescentes ante las pantallas", Colección Generaciones Interactivas-Fundación Telefónica, Madrid, 2011.

dio en todas las edades, con sus amigos un 27,5% de niños y niñas comprendidos entre 6 y 9 años y un 38,5% los niños, niñas y adolescentes entre 10 y 18 años; con sus padres apenas un 18,5% los niños y niñas comprendidos entre 6 y 9 años y un 9,25% y los niños, niñas y adolescentes entre 10 y 18 años (p. 212).

El 49% de niños y niñas comprendido entre 6 y 9 años visitan páginas web, el 34% comparten videos, fotos y presentaciones, 14% usan el correo electrónico, descargan música un 23%, chatean o usan el Messenger un 18%, usan el Facebook y otras redes sociales un 18,5%. El 57,5% de niños, niñas y adolescentes entre 10 y 18 años visitan páginas web, envían SMS un 26,5%, comparten videos, fotos y presentaciones un 38,5%, usan el correo electrónico un 43,5%, descargan música, películas o programas un 42,5%, 62,5% usan el Facebook y otras redes sociales, un 67% juegan en red (mayoritariamente son hombres con un 63%), hablan por Skype o similares un 13%, un 8% crean blogs, 5% fotologs 5%, 25,5% web/blog y, un 2,5% compran o venden (pp. 212 y 213).

En cuanto a la percepción del riesgo es posible identificar diferencias importantes en función de la edad y el sexo de los entrevistados: pondrían cualquier foto o video en Internet a los 10 años o menos un 18,5% a los 11 un 13,5%, a los 12 un 19% de los varones y un 13% de las chicas, a los 13 años un 21%, a los 14 años un 24% los chicos y un 19% las chicas, a los 15 años un 24% de los chicos y un 13% las chicas, a los 16 años un 27% los chicos y un 17% las chicas, a los 17 años un 39% los chicos y un 19% las chicas (p. 213).

Consideran que "es divertido hablar con desconocidos a través de internet"a los 10 años o menos un 10% de los chicos y un 4% de las chicas, a los 11 un 9% de los chicos y un 6% de las chicas, a los 12 años un 5% de los chicos y un 4% de las chicas, a los 13 años un 13% de los chicos y un 9% de las chicas, a los 14 años un 16% de los chicos y un 13% de las chicas, a los 15 años un 20% de los chicos y un 10% de las chicas, a los 16 años un 19% de los chicos y un 15% de las chicas, a los 17 años un 28% de los chicos y un 11% de las chicas (p. 214).

No les importa agregar desconocidos al Messenger a los 10 años o menos a un 4% de los chicos y un 8% de las chicas, a los 11 a un 9% de los chicos y un 4% de las chicas, a los 12 años a un 3% de los chicos y un 4% de las chicas, a los 13 año un 12% de los chicos y un 5% de las chicas, a los 14 años un 18% de los chicos y un 10% de las chicas, a los 15 años a un 16% de los chicos y un 9% de las chicas, a los 16 años un 11% de los chicos y un 8% de las chicas, a los 17 años un 25% de los chicos y un 6% de las chicas (p. 214).

Como se puede concluir, los varones tienen una propensión mayor a realizar actividades riesgosas; sin embargo, es común el compartir información que puede afectar su vida privada.

A nivel global, en datos más recientes (de Livingstone y Haddon, 2009, p. 16[9]), se reporta que la principal amenaza que enfrentan los NNA en línea es la revelación de información personal sensible, un tercio de los adolescentes acceden a contenidos violentos, *ciberbullying* en uno de cada cinco adolescentes, el contacto con personas desconocidas que entrañan algún peligro un 9%, en menor número reportan las amenazas en línea o sentirse inseguros por el contacto.

2. La regulación de internet: un enfoque de derechos

En la era digital, cualquier análisis de los derechos de la infancia debe considerar como un elemento fundamental el contenido de la Convención sobre los Derechos del Niño[10], instrumento[11] aprobado en los albores del internet que brinda un marco relevante para establecer las orientaciones que deberían desarrollarse en las políticas públicas y en la normativa referida al acceso y uso del internet con un enfoque de derechos.

Lo primero es el reconocimiento de que los NNA son sujetos plenos de derechos y que pueden ejercerlos de forma progresiva de acuerdo a su edad y madurez (art. 5), en un contexto de integralidad e interdependencia de los derechos, lo que

---

9 Datos de Livingstone y Haddon en el estudio ya citado.

10 La amplia ratificación de la CDN ha llevado a que la Corte Interamericana de Derechos Humanos afirme que existe un *corpus juris* sobre derechos de los niños, niñas y adolescentes y que forma parte de este la Convención sobre los Derechos del Niño, la cual ha sido ratificada por todos los estados miembros latinoamericanos (en realidad por todos los estados americanos excepto Estados Unidos). Este comprensivo "(…) *corpus juris* del Derecho Internacional de los Derechos Humanos está formado por un conjunto de instrumentos internacionales de contenido y efecto jurídico distintos (tratados, convenios, resoluciones y declaraciones); así como las decisiones adoptadas por los órganos internacionales. Su evolución dinámica ha ejercido un impacto positivo en el Derecho Internacional, en el sentido de afirmar y desarrollar la aptitud para regular las relaciones entre los Estados y los seres humanos bajo sus respectivas jurisdicciones" (Corte Interamericana de Derechos Humanos, *El Derecho a la Información sobre la Asistencia Consular en el Marco de las Garantías del Debido Proceso Legal,* Opinión Consultiva OC-16/99 de 1 de octubre de 1999, Serie A, No. 16, párrafo 115). En lo que se refiere al tema materia del presente trabajo la OC-17 (ya citada) en su párrafos 37 y 53; en los casos: de los "Niños de la Calle" (ya citado) en su párrafo 194; *Instituto de Reeducación del Menor*, en la Sentencia de 2 de septiembre de 2004, publicada en la Serie C, No. 12, párrafo 148; *Hermanos Gómez Paquiyauri*, en la Sentencia de 8 de junio del 2004, párrafo 156 se reconoce esto "Tanto la Convención Americana como la Convención sobre los Derechos del Niño forman parte de un muy comprensivo *corpus juris* internacional de protección de los niños que debe servirá esta Corte para fijar el contenido y los alcances de la disposición general definida en el artículo 19 de la Convención Americana".

11 Por citar algunos de los más relevantes: Committee on the Rights of the Children, Report of the 2014 Day of General Discussion «Digital media and children's rights, Geneva, 2014, disponible en línea http://www.ohchr.org/Documents/HRBodies/CRC/Discussions/2014/DGD_report.pdf; Third, Amanda, et. al., Children Rights's in the Digital Age: A download from children around the world, Young and Well Cooperative Research Centre, Melbourne, 2014; Pavez, María Isabel, Los derechos de la infancia en la era de Internet, CEPAL/UNICEF, Serie Políticas Sociales No. 210, 2014; UNICEF, Centro de Investigaciones Innocenti, La seguridad de los niños en línea: retos y estrategias mundiales, Florencia, 2012.

demanda mantener un enfoque equilibrado entre las necesidades derivadas de la protección especial[12] y la condición de sujetos plenos de derechos.

Los derechos que componen el marco general para interpretar los derechos de la infancia y adolescencia son: el derecho a acceder a información (art. 17); la libertad de expresión (art. 13); el derecho a su vida privada (art. 16); el derecho a la opinión (art. 12); el derecho a la identidad (art. 8); el derecho a la educación (art. 28) y el derecho al descanso y esparcimiento, al juego y a las actividades recreativas propias de su edad (art. 31).

Estos derechos están relacionados directamente con el internet y con la niñez y juventud, por tanto, deben considerarse, en conjunto, como parte de las disposiciones que determinan las obligaciones que tienen los progenitores en la crianza de sus hijos (art. 18), la responsabilidad de la familia como guía en el ejercicio de sus derechos (art. 5) y las obligaciones estatales para asegurarles protección contra toda forma de perjuicio, abuso físico o mental y explotación (artículos 19, 32, 34).

El artículo 17 de la CDN, a propósito de los medios de comunicación tradicionales (disposición plenamente aplicable al internet), reconoce el derecho de los niños a acceder a información y materiales procedentes de diversas fuentes, en especial, pero no exclusivamente, aquellos que tengan por finalidad promover su bienestar social, espiritual y moral y su salud física y mental. Las obligaciones específicas de los estados son: promover la producción e intercambio (a nivel nacional e internacional) de material de interés social y cultural para el niño, considerando las necesidades lingüísticas de los niños pertenecientes a grupos minoritarios o indígenas y la elaboración de directrices para protegerles de información y material perjudiciales[13].

---

12 "Teniendo presente que la necesidad de proporcionar al niño una protección especial ha sido enunciada en la Declaración de Ginebra de 1924 sobre los Derechos del Niño y en la Declaración de los Derechos del Niño adoptada por la Asamblea General el 20 de noviembre de 1959 y reconocida en la Declaración Universal de Derechos Humanos, en el Pacto Internacional de Derechos Civiles y Políticos (en particular, en los artículos 23 y 24), en el Pacto Internacional de Derechos Económicos, Sociales y Culturales (en particular, en el artículo 10) y en los estatutos e instrumentos pertinentes de los organismos especializados y de las organizaciones internacionales que se interesan en el bienestar del niño…". Preámbulo de la CDN.

13 "Los Estados Partes reconocen la importante función que desempeñan los medios de comunicación y velarán por que el niño tenga acceso a información y material procedentes de diversas fuentes nacionales e internacionales, en especial la información y el material que tengan por finalidad promover su bienestar social, espiritual y moral y su salud física y mental. Con tal objeto, los Estados Partes:

a) Alentarán a los medios de comunicación a difundir información y materiales de interés social y cultural para el niño, de conformidad con el espíritu del artículo 29;

b) Promoverán la cooperación internacional en la producción, el intercambio y la difusión de esa información y esos materiales procedentes de diversas fuentes culturales, nacionales e internacionales;

c) Alentarán la producción y difusión de libros para niños;

El artículo 13 reconoce la libertad de expresión de cada niño, niña y adolescente, por ello, puede buscar, recibir y difundir informaciones e ideas de todo tipo, sin consideración de fronteras, ya sea oralmente, por escrito o impresas, en forma artística o por cualquier otro medio elegido por el niño; ese derecho puede ser restringido, mediante una ley, siempre que esas restricciones estén dirigidas al respeto de los derechos o a la reputación de los demás y a la protección de la seguridad nacional o el orden público, para proteger la salud o la moral públicas.

El artículo 16 prohíbe las injerencias arbitrarias e ilegales en la vida privada, familia, domicilio, correspondencia de los NNA, así como los ataques ilegales contra su honra y reputación.

El artículo 12 establece que todos los NNA, en condiciones de formarse un juicio propio, tienen el derecho de expresar su opinión libremente en los asuntos que les afecten y que esas opiniones pueden ser debidamente tomadas en cuenta en función de su edad y madurez.

Adicionalmente, las TIC's se encuentran relacionadas con los derechos a la educación[14]; a la recreación, al uso del tiempo libre y al juego, la vida cultural y artística[15]; y a la identidad[16].

Son sus progenitores (ambos padres en términos de la Convención) los que tienen la obligación primordial en la crianza, cuidado y desarrollo del niño (art. 18);

---

d) Alentarán a los medios de comunicación a que tengan particularmente en cuenta las necesidades lingüísticas del niño perteneciente a un grupo minoritario o que sea indígena;

e) Promoverán la elaboración de directrices apropiadas para proteger al niño contra toda información y material perjudicial para su bienestar, teniendo en cuenta las disposiciones de los artículos 13 y 18.

14 Artículo 28.1 "Los Estados Partes reconocen el derecho del niño a la educación y, a fin de que se pueda ejercer progresivamente y en condiciones de igualdad de oportunidades ese derecho…"

15 Artículo 31.1 "Los Estados Partes reconocen el derecho del niño al descanso y el esparcimiento, al juego y a las actividades recreativas propias de su edad y a participar libremente en la vida cultural y en las artes".

16 Artículo 8.1 "Los Estados Partes se comprometen a respetar el derecho del niño a preservar su identidad, incluidos la nacionalidad, el nombre y las relaciones familiares de conformidad con la ley sin injerencias ilícitas". Se considera que este derecho, además de los elementos referidos en la norma citada tiene un "…componente dinámico y flexible donde otros aspectos tan cotidianos como las relaciones sociales, lugares, roles, entre otras, van dejando rastro y, a su vez, moldeando la identidad de una persona. Se trata de un continuo posicionamiento siempre en conflicto y nunca completo. Esto implica que cambio, diferencias contradicciones son algunos de los componentes de la identidad, subrayando cuán complejo es el concepto. Lo que importa rescatar es que el proceso de conformación de la identidad deja la puerta abierta a nuevos contextos y situaciones que van contribuyendo a la identidad. Aquí es donde entra en juego el rol de las nuevas tecnologías, puesto que a nivel general implica un cambio de contexto social y cultural; y a nivel específico, un cambio en la forma en que niños, niñas y adolescentes y jóvenes se relacionan entre ellos y se presentan al mundo a través de perfiles *on line*, lo que va dejando huella en sus construcciones identitarias". Pavez, M. I., Los derechos de la infancia en la era de Internet: América Latina y las nuevas tecnologías, Cepal-Unicef, Cepal, Serie Políticas Sociales No. 210, Santiago, 2014.

el Estado es responsable de tomar todas las medidas necesarias, sean legislativas, administrativas, sociales y educativas para proteger al niño contra toda forma de perjuicio o abuso físico o mental, descuido o trato negligente, malos tratos o explotación, incluido el abuso sexual (art. 19).

Las normas citadas deben ser leídas en conjunto con dos de los principios claves de la CDN[17]: no discriminación (art. 2[18]) e interés superior (art. 3.1[19]). Además, debe considerarse la regla del art. 5 del instrumento que introduce un concepto clave en materia de derechos de infancia y adolescencia: el ejercicio progresivo de los derechos[20].

En el "Día de Debate General" del CRC sobre "Medios digitales y derechos de la infancia" que tenía como objetivo central analizar los efectos de las TIC's en la infancia, con una estrategia basada en los derechos, se estableció la necesidad de incrementar las oportunidades de acceso a las TIC's, protegiéndolos de los posibles daños sin limitar sus beneficios; en particular porque es "difícil separar la vida *on line* y *off line*" (CRC, 2014, párr. 11) al ser el internet parte de su vida cotidiana (párr. 45). Limitar el acceso o no dar una educación digital adecuada es una violación a los derechos que produce una serie de consecuencias negativas que, a su vez, surgen al privarles de los beneficios que su uso brinda, lo que además tiene como consecuencia el incremento en la brecha entre el Norte y el Sur (párr. 15) y la exclu-

17 CRC. Observación General No. 5 (2003). Medidas generales de aplicación de la Convención sobre los Derechos del Niño (artículo 4 y 42 y párrafo 6 del artículo 44).Documento CRC/GC/2003/5.

18 1. Los Estados Partes respetarán los derechos enunciados en la presente Convención y asegurarán su aplicación a cada niño sujeto a jurisdicción, sin distinción alguna, independientemente de la raza, el color, el sexo, el idioma, la religión, la opinión política o de otra índole, el origen nacional, étnico o social, la posición económica, los impedimentos físicos, el nacimiento o cualquier otra condición del niño, de sus padres o de sus representantes legales.
2.Los Estados Partes tomarán todas las medidas apropiadas para garantizar que el niño se vea protegido contra toda forma de discriminación o castigo por causa de la condición, las actividades, las opiniones expresadas o las creencias de sus padres, de sus tutores o de sus familiares."

19 "...En todas las medidas concernientes a los niños, que tomen las instituciones públicas o privadas de bienestar social, los tribunales, las autoridades administrativas o los órganos legislativos una consideración primordial a que se atenderá será el interés superior del niño..."

20 El "ejercicio progresivo" o "evolución de las facultades" ha sido descrito como un nuevo principio de interpretación del derecho internacional y, por tanto, de los derechos de infancia y adolescencia, según el cual se reconoce que, a medida que los niños van adquiriendo competencias cada vez mayores, se reduce su necesidad de orientación y aumenta su capacidad de asumir responsabilidades respecto a las decisiones que afectan sus vidas. A propósito de esto se puede revisar Gerison Lansdown. La evolución de las facultades del niño. UNICEF-Save the Children: Centro de Investigaciones Innocenti. Florencia-Italia. s/f.

sión de grupos de niños, en especial de los que están en situación de vulnerabilidad y marginación (párr. 31).

El principio que debe guiar toda acción es el de "igual acceso" para todos los NNA (párr. 59), su aplicación podría impedir que en nombre de la protección se incremente la censura y el control. Un enfoque de este tipo que debe ser considerado contrario a los derechos humanos (párr. 15).

El CRC asume así que los riesgos en las TIC's no son intrínsecos (Pavez, 2014, p. 37), se presentan de la misma forma que en cualquier otro espacio público, pero existen: acoso y abuso sexual en línea, explotación sexual o laboral (por medio de la conocida captación en línea o *groomig*), pornografía, violaciones al derecho a la privacidad, estafas, fácil acceso a información inadecuada o violenta, contenidos sexuales autogenerados (CRC, párr. 66), acoso u hostigamiento en línea. Sin embargo, se considera que los aspectos positivos son mayores, por ello, cualquier enfoque basado en la restricción o limitación de acceso debe rechazarse, la complejidad de la red implica tomar medidas tecnológicas, legislativas, formativas y de sensibilización que involucren a todos: niños y niñas (cuya voz, participación y punto de vista es esencial), progenitores, familia, otros usuarios, maestros, proveedores de internet, autoridades, etc. Todo lo anterior junto con la participación de la sociedad civil, la familia y la industria. La persecución a quienes cometen delitos es clave, además de un acompañamiento efectivo a las víctimas que incluye la reparación integral de sus derechos (CRC, párr. 44 a 110).

3. Regulación internacional de internet y la niñez y adolescencia

En el contexto americano, no existe instrumento internacional de carácter específico en esta materia. Es claro que los instrumentos de carácter general, como la CADH, CDN y su Protocolo Facultativo sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía del año2000, el Protocolo para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres y niños, que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional ("Protocolo de Palermo", 2000) son plenamente aplicables, esto a diferencia de lo que sucede en Europa, donde se aprobó el Convenio del Consejo de Europa sobre la Ciberdelincuencia (2001) y el Convenio del Consejo de Europa sobre la protección de los niños contra la explotación y el abuso sexual (2007).

De forma más reciente -año 2011- la Unión Europea adoptó la Directiva del Parlamento Europeo y del Consejo relativa a la lucha contra los abusos sexuales, la explotación sexual de los niños y la pornografía infantil, que considera como delito a los abusos y a la explotación sexual, a la captación o seducción de niños con fines sexuales, a los espectáculos pornográficos en línea y la exhibición de imágenes

de abusos sexuales infantiles sin descargar ficheros; además, se garantiza que los delincuentes ciudadanos de la Unión Europea serán enjuiciados por delitos cometidos en el exterior de la Unión Europea; concede asistencia, apoyo y protección a los niños víctimas de los delitos contemplados, incluida la reclamación de indemnizaciones; se incluye la creación de un sistema de intercambio de datos sobre condenas a delincuentes sexuales entre las autoridades y se permite la remoción obligatoria y el bloqueo opcional de sitios web con contenidos de abusos sexuales infantiles [21].

En el ámbito Europeo son muy importantes los esfuerzos de autorregulación, por ejemplo, la Comisión Europea promovió los «Principios para redes sociales más seguras de la Unión Europea», en los que se ha puesto énfasis en la necesidad de asegurar la configuración de privacidad, así como la educación, sensibilización y denuncia de abusos sexuales. Basándose en estos principios se evalúa a los proveedores de forma periódica[22].

En el ámbito regional se destaca el «Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes» llamado «Memorando de Montevideo»[23], este documento es el resultado del trabajo de un grupo de personas, algunas de ellas representantes de instituciones públicas y privadas como: el Instituto de Investigaciones para la Justicia (IIJ), el Instituto Federal de Acceso a la Información de México (IFAI), la Agencia de Protección de Datos de Uruguay, la Agencia de Protección de Datos de Cataluña, la Agencia (Comisariado) de Protección de Datos de Canadá, la Secretaría Especial de Derechos Humanos de Brasil, UNICEF, el Instituto Interamericano de Derechos del Niño, así como jueces de infancia y académicos en tecnologías de la información, derechos humanos y derechos de la infancia y adolescencia, con el apoyo del Centro Internacional de Investigaciones para el Desarrollo de Canadá, redactado en el año 2009. Todas estas instituciones redactaron, en el año 2009, un importante documento que contiene una serie de recomendaciones en materia de prevención y educación de niñas, niños y adolescentes; reformas legales; aplicación de las leyes por parte del Estado; políticas públicas y recomendaciones para la industria.

Si bien el documento no es obligatorio ha tenido un impacto relevante, por

21Unión Europea, Actos legislativos y otros instrumentos – Directiva del Parlamento Europeo y del Consejo relativo a la lucha contra los abusos sexuales, la explotación sexual de los niños y la pornografía infantil, por la que se deroga la Decisión marco 2004/68/JAI, Unión Europea, Bruselas, 4 de noviembre de 2011.

22 UNICEF, Centro de Investigaciones Innocenti, La seguridad de los niños en línea. Retos y estrategias mundiales, Florencia, 2012, p. 11.

23 El texto completo del "Memorando de Montevideo" se encuentra disponible en http://clicseguro.sep.gob.mx/archivos/Memorandum_Montevideo.pdf .

ejemplo, la Corte Constitucional Colombiana[24] usó el documento para resolver un caso de violación del derecho a la privacidad, por parte de un progenitor que creó una cuenta de Facebook a nombre de su hija de 4 años.

4. Normativa ecuatoriana

4.1. El marco normativo general ecuatoriano

La Constitución de la República[25] recoge los principios y derechos de la CDN y el CNA.

En términos generales, el marco normativo nacional es similar al internacional, sin embargo, los dos instrumentos nacionales, por el tiempo de su aprobación, ya recogen algunas disposiciones relacionadas a las TIC's.

En la Constitución de 2008 se reitera la regla general de que «…niñas, niños y adolescentes gozarán de los derechos comunes del ser humano, además de los específicos de su edad» (art. 45); el reconocimiento de su calidad de sujetos plenos de derechos; los principios de ejercicio progresivo y el interés superior y la prevalencia de los derechos (artículos 44 a 46). En la Constitución se define al desarrollo integral como «proceso de crecimiento, maduración y despliegue del intelecto, capacidades, potencialidades y aspiraciones, en un entorno familiar, escolar, social y comunitario de afectividad y seguridad, de cadaNNA».

Todas las personas tienen derecho «a la intimidad personal y familiar» (art. 66.20), el derecho a guardar reserva sobre las convicciones, por ello, no se puede utilizar sin autorización del titular o de sus legítimos representantes, la información personal o de terceros sobre sus creencias religiosas, filiación o pensamiento político ni sobre datos referentes a su salud y vida sexual, salvo por necesidades de atención médica (número 11), la protección de la imagen y la voz de la persona (número 18), la inviolabilidad y el secreto de la correspondencia física y virtual, la que no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley y con autorización judicial (número 21).

De forma específica, se determina la obligación de proteger a niños, niñas y adolescentes de «(...) la influencia de programas o mensajes, difundidos a través de cualquier medio, que promuevan la violencia, o la discriminación racial o de género(…)» (art. 46.7).

En lo referido a la comunicación y a las tecnologías de la información se establece como derecho, individual o colectivo, el «(…) acceso universal a las tecnologías de información y comunicación» (artículo 16.2); siendo una obligación del Estado,

24 Corte Constitucional Colombiana, sentencia T-260/12, disponible en http://www.corteconstitucional.gov.co/relatoria/2012/T-260-12.HTM

25 Registro Oficial No. 449 de 20 de octubre de 2008.

en el marco del fomento de la pluralidad y diversidad de la comunicación, facilitar ese acceso universal, en particular «para aquellas personas y colectividades que carezcan de dicho acceso o lo tengan de forma limitada» (art. 17.2).

El Estado central tiene competencia exclusiva para regular y controlar el «(...) espectro radioeléctrico y el régimen general de comunicaciones y telecomunicaciones» (art. 261.10); se lo considera un sector estratégico (inciso final artículo 313) y un servicio público que debe ser provisto por el Estado[26] (art. 314). Estableciéndose como obligatorio el «Incorporar las tecnologías de la información y comunicación en el proceso educativo y propiciar el enlace de la enseñanza con las actividades productivas o sociales» (art. 347.8).

El Código de la Niñez y Adolescencia[27], un instrumento pre Constitución, aprobado para compatibilizar la legislación interna con el contenido y principios de la CDN, regula el derecho a la vida privada en los siguientes términos: « (...) niños, niñas y adolescentes tienen derecho a que se respete la intimidad de su vida privada y familiar; y la privacidad e inviolabilidad de su domicilio, correspondencia y comunicaciones telefónicas y electrónicas, de conformidad con la ley». Sin embargo, en ese cuerpo normativo se introduce una posible restricción adicional al derecho, ya que se afirma que este derecho se reconoce «sin perjuicio de la natural vigilancia de padres y maestros[28]».

Esta disposición debe entenderse en el contexto del conjunto de derechos y principios que la legislación ecuatoriana reconoce para los NNA, por ello, no puede interpretarse como un cheque en blanco que habilita a los progenitores y maestros a revisar e intervenir en la correspondencia y en las comunicaciones telefónicas y electrónicas de hijos y pupilos; esto debe conciliarse con el reconocimiento de su calidad de sujetos plenos de derechos y con el ejercicio progresivo (art. 13 Código de la Niñez y Adolescencia), en el que se determina que:

> «El ejercicio de los derechos y garantías y el cumplimiento de los deberes y responsabilidades de niños, niñas y adolescentes se harán de manera progresiva, de acuerdo a su grado de desarrollo y madurez. Se prohíbe cualquier restricción al ejercicio de estos derechos y garantías que no esté expresamente contemplado en este Código».

---

26 El Estado garantizará que los servicios públicos y su provisión respondan a los principios de obligatoriedad, generalidad, uniformidad, eficiencia, responsabilidad, universalidad, accesibilidad,regularidad, continuidad y calidad. El Estado dispondrá que los precios y tarifas de los servicios públicos sean equitativos, y establecerá su control y regulación». Segundo inciso del artículo 314.

27 Código de la Niñez y Adolescencia, artículo 53, ley publicada en Registro Oficial No. 737 de 3 de enero del 2003.

28 Art. 53 CNA

En mi opinión, el límite para aceptar esta «vigilancia» sería la adolescencia, a partir de los 12 años se debería obtener autorización del propio adolescente o de una autoridad judicial para que progenitores o maestros pueden «vigilar» las comunicaciones.

La Ley Orgánica de Telecomunicaciones (Registro Oficial Suplemento 439 de 18-feb.-2015) contiene el marco legal aplicable a internet, sin normas específicas referidas a menores de edad y las redes sociales; sus disposiciones, obviamente, son aplicables a ellos. Las más relevantes se encuentran en los "Derechos de los abonados, clientes y usuarios" (art. 22) y en las "Obligaciones de los prestadores de servicios de telecomunicaciones" (art. 23).

En cuanto a los derechos (art. 22) se reconoce "(...) el secreto e inviolabilidad del contenido de sus comunicaciones, con las excepciones previstas en la Ley" (numeral 3); "la privacidad y protección de sus datos personales, por parte del prestador con el que contrate servicios, con sujeción al ordenamiento jurídico vigente" (numeral 4) y la neutralidad de la red y el derecho a recibir e intercambiar información en los siguientes términos:

> "(...) acceder a cualquier aplicación o servicio permitido disponible en la red de internet. Los prestadores no podrán limitar, bloquear, interferir, discriminar, entorpecer ni restringir el derecho de sus usuarios o abonados a utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación, desarrollo o servicio legal a través de internet o en general de sus redes u otras tecnologías de la información y las comunicaciones, ni podrán limitar el derecho de un usuario o abonado a incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos en la red, siempre que sean legales. Se exceptúan aquellos casos en los que el cliente, abonado o usuario solicite de manera previa su decisión expresa de limitación o bloqueo de contenidos, aplicaciones, desarrollos o servicios disponibles o por disposición de autoridad competente. Los prestadores pueden implementar las acciones técnicas que consideren necesarias para la adecuada administración de la red en el exclusivo ámbito de las actividades que le fueron habilitadas, para efectos de garantizar el servicio (...)".

En lo referido a los deberes (art. 24) de los "Prestadores de Servicios de Telecomunicaciones" (con independencia del título habilitante del mismo), los más relevantes son: "garantizar el acceso igualitario y no discriminatorio a cualquier persona que requiera sus servicios" (número 1); "garantizar el secreto e inviolabilidad de las comunicaciones cursadas a través de las redes y servicios de telecomunicaciones, sin perjuicio de las excepciones establecidas en las leyes (número 13); "adoptar las medidas necesarias para la protección de los datos personales de sus usuarios y abonados, de conformidad con esta Ley, su Reglamento General y las normas técnicas y regulaciones respectivas (número 14) y

> "No limitar, bloquear, interferir, discriminar, entorpecer, priorizar ni restringir el derecho de sus usuarios o abonados a utilizar, enviar, recibir u ofrecer

> cualquier contenido, aplicación, desarrollo o servicio legal a través de Internet o en general de sus redes u otras tecnologías de la información y las comunicaciones, ni podrán limitar el derecho de un usuario o abonado a incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos en la red, siempre que sean legales, salvo las excepciones establecidas en la normativa vigente. Se exceptúan aquellos casos en los que el cliente, abonado o usuario solicite de manera previa su decisión expresa de limitación o bloqueo de contenidos, o por disposición de autoridad competente. Los prestadores pueden implementar las acciones técnicas que consideren necesarias para la adecuada administración de la red en el exclusivo ámbito de las actividades que le fueron habilitadas para efectos de garantizar el servicio" (número 17).

De las disposiciones citadas es claro el reconocimiento expreso (en la Ley de Telecomunicaciones) de que todas las personas tienen el derecho a acceder sin discriminación a los servicios de internet; el secreto y la privacidad de las comunicaciones (en cualquier forma que estás se presenten); la privacidad y protección de los datos personales; la libertad para enviar, recibir u ofrecer cualquier contenido, aplicación, desarrollo o servicio legal y la neutralidad de la red. En lo referido a la privacidad y secreto de las comunicaciones, la protección de los datos personales y el bloqueo o limitación de ciertos contenidos, pueden hacerse por disposición de acuerdo con la ley.

Llama la atención, en los primeros casos (privacidad de las telecomunicaciones y protección de datos personales), se establezca de forma expresa que cualquier limitación debe ser hecha de "acuerdo con la ley", y para la limitación o bloqueo de contenidos, únicamente se establece que esto se podrá hacer por "disposición de la autoridad competente" o por pedido del cliente, abonado o usuario. El pedido de bloqueo podría hacerlo quien contrata el servicio, es decir, los representantes legales de los menores de edad.

La LOT no contiene disposiciones referidas directamente a NNA, pero su texto es plenamente aplicable a ellos. En lo que se relaciona con su capacidad legal, los derechos y su ejercicio, la posible responsabilidad penal y el rol de los progenitores en la guía de sus derechos, es necesario referirse a las reglas de carácter general.

4.2. Capacidad legal

La capacidad legal de una persona es la posibilidad de que una persona se obligue por sí misma y sin el ministerio o representación de otra. En esta materia, la regla general es la contenida en el Código Civil, en el que se mantiene la diferencia entre menores de edad, es decir, impúberes (mujeres menores de 12 años y varones menores de 14 años), los que son incapaces absolutos y, por tanto, sus actos no surten ni siquiera obligaciones naturales; y púberes (varones mayores de 14 y mujeres de más de 12 años), los que son incapaces relativos, sus actos pueden surtir efectos en determinadas circunstancias (art. 1463)

Por ello la capacidad legal debe ser examinada en cuanto a la posibilidad de NNA de celebrar contratos para acceder a servicios de internet o de aceptar las condiciones de uso de las redes sociales.

Como se puede colegir de las reglas del Código Civil (CC), los menores de edad impúberes no estarían habilitados para adherirse a los contratos de los diferentes servicios en línea, en el caso de los púberes estos dependerían la ratificación (expresa o tácita) por parte de sus representantes legales o que los servicios sean contratados en el marco de la administración de su peculio profesional o industrial (CC art. 288), para cuyos efectos son considerados mayores de edad. De igual forma, tienen capacidad legal para comparecer en defensa de sus derechos, sin necesidad de ser autorizados o representados, los adolescentes, en términos del Código de la Niñez y Adolescencia (CNA). Los niños y niñas que deben acudir a juicio y ser representados por sus progenitores, en caso de que la acción judicial sea contra sus progenitores, pueden pedir «auxilio» (art. 65 CNA). También pueden acudir directamente en defensa de sus derechos en todos los casos en que puedan contratar válidamente, esto de acuerdo a lo dispuesto en el art.

4.3. Ejercicio progresivo

La capacidad de ejercicio directo de ciertos derechos, que por su naturaleza son personalísimos, difiere de la regla de la capacidad legal, ya que esto depende de su desarrollo y madurez. En el artículo 13 del CNA esto se encuentra formulado de la siguiente manera: «El ejercicio de los derechos y garantías y el cumplimiento de los deberes y responsabilidades de niños, niñas y adolescentes se harán de manera progresiva, de acuerdo a su grado de desarrollo y madurez. Se prohíbe cualquier restricción al ejercicio de estos derechos y garantías que no esté expresamente contemplado en este Código». La consideración en cuanto al uso del Internet estaría ligado a sus capacidades personales, en tanto este material no sea perjudicial para su interés superior y desarrollo.

En la legislación ecuatoriana, en el CNA se establece una diferencia entre niñez y adolescencia, ya que estas son categorías diferentes a las del CC. Niños y niñas son todas las personas hasta los 12 años, en tanto que adolescentes son aquellas personas entre 12 y 18 años. Esta diferencia es relevante, ya que a los niños y niñas se les da un margen menor de decisión que a los adolescentes, estos últimos, incluso, deben otorgar su consentimiento para la adopción, son responsables penalmente y pueden elegir el progenitor con el que van a vivir en caso de separación de sus padres, esto lleva a la conclusión de que la relación que se establece entre los adultos y adolescentes es diferente y, por tanto, sus puntos de vista y opiniones deberán ser valoradas de manera diferente, algo que redunda en el ejercicio de los derechos.

4.4. Derecho a la información

En términos generales, el artículo 45 reconoce el derecho de todo niño, niña y adolescente a

> «buscar y escoger información; y a utilizar los diferentes medios y fuentes de comunicación, con las limitaciones establecidas en la ley y aquellas que se derivan del ejercicio de la patria potestad. Es deber del Estado, la sociedad y la familia, asegurar que la niñez y adolescencia reciban una información adecuada, veraz y pluralista; y proporcionarles orientación y una educación crítica que les permita ejercitar apropiadamente los derechos señalados».

En este artículo, el legislador introdujo una restricción adicional al ejercicio del derecho a la información y añadió, además de las limitaciones legales, la frase: «aquellas que se deriven del ejercicio de la patria potestad», habilitando, así, a los progenitores para que controlen la información que reciben los NNA; en todo caso, esta regla debe ser leída en conjunto con la del ejercicio progresivo, de forma tal que, la intervención no sea de tal naturaleza que limite el ejercicio indebidamente. Es en el artículo 46 del CNA que se establece la prohibición general de acceso a «imágenes, textos o mensajes inadecuados para su desarrollo»; en el penúltimo inciso del artículo 47 se establece qué tipo de mensajes afectarían el desarrollo de los niños, niñas y adolescentes:

> «los textos, imágenes, mensajes y programas que inciten a la violencia, exploten el miedo o aprovechen la falta de madurez de los niños, niñas y adolescentes para inducirlos a comportamientos perjudiciales o peligrosos para su salud y seguridad personal y todo cuanto atente a la moral o el pudor».

En tanto que se consideran beneficiosos para sus derechos, y por tanto, debería fomentarse la difusión, «materiales de interés social y cultural» (art. 47).

4.5. Libertad de expresión

En cuanto a la libertad de expresión, el artículo 59 del CNA se encuentra formulado en términos muy parecidos a la CDN:

> «Los niños, niñas y adolescentes tienen derecho a expresarse libremente, a buscar, recibir y difundir informaciones e ideas de todo tipo, oralmente, por escrito o cualquier otro medio que elijan, con las únicas restricciones que impongan la ley, el orden público, la salud o la moral públicas, para proteger la seguridad, derechos y libertades fundamentales de los demás».

La redacción del artículo, erradamente parece diferenciar la imposición de restricciones por la ley, el orden público, la salud, la moral pública y, para proteger la seguridad, derechos y libertades de los demás; en correspondencia con las normas

internacionales en la materia[29], la restricción debería constar en una ley y estar destinada únicamente a los objetivos legítimos que podrían habilitar a la restricción del derecho. Esta regla habilitaría a que los progenitores, en realidad, los adultos a cargo del cuidado de niños, niñas y adolescentes, soliciten -de acuerdo a lo previsto en la LOT- el bloqueo de acceso a ciertas páginas de internet; sin embargo, es claro que por el derecho a ser consultados en todos los asuntos que les afectan, esto de acuerdo al desarrollo y madurez del niño, niña o adolescente, en cumplimiento de lo previsto en el artículo 60 del mismo CNA.

4.6. Derecho a la vida privada y protección de datos personales

El CNA, en su artículo 53, recoge este derecho de la siguiente forma:

> «Sin perjuicio de la natural vigilancia de los padres y maestros, los niños, niñas y adolescentes tienen derecho a que se respete la intimidad de su vida privada y familiar; y la privacidad e inviolabilidad de su domicilio, correspondencia y comunicaciones electrónicas, de conformidad con la ley, prohibiéndose las «injerencias arbitrarias o ilegales en su vida privada».

El legislador incluyó la idea de «la natural vigilancia de los padres y maestros» que no tiene correspondencia alguna con los textos internacionales de la materia y se añadió una restricción a los derechos que podría aplicarse de forma abusiva. Sin desconocer la potestad que tienen los progenitores de guiar a los niños, niñas y adolescentes (NNA) en el ejercicio de sus derechos y, en este marco tener acceso a ciertas comunicaciones cuando sus hijos e hijas son más pequeños, no parece que introducir la idea de «natural vigilancia» sea compatible con la noción de ejercicio y autonomía progresiva, por esto, el texto debería ser interpretado de forma que pueda conciliarse con la condición de sujeto pleno de derechos de los menores de edad y el ejercicio progresivo de los derechos, particularmente en la adolescencia, en la que la autonomía es mayor.

El caso de los maestros es más complejo aún, no parece que se encuentren habilitados, en caso alguno, para vigilar las comunicaciones de los estudiantes, es decir, no podría admitirse que esta regla sea usada para que se acceda, sin autorización, a la correspondencia o a cualquier clase de comunicación telefónica o electrónica de sus estudiantes.

Incluso, en el caso de los progenitores, debería demostrarse que la intervención es necesaria por el interés superior de su hijo o hija, lo que requiere una justificación caso por caso, incluso, esto no sería admisible en el caso de comunicaciones de NNA con mayor edad y madurez. Esa intervención requiere de una evaluación, caso por caso, de necesidad, razonabilidad y proporcionalidad; en caso de no cumplir esas condiciones, la intervención se tornaría en arbitraria. En el caso de los maestros, no debería existir esta posibilidad por regla general, la excepción estaría relacionada a ciertos casos de gravedad o urgencia debidamente justificados.

29 Convención Americana de Derechos Humanos.

En la Constitución, la protección a este derecho se hace de forma más general: «Se reconoce y garantizará a las personas… [e]l derecho a la intimidad personal y familiar» (art. 66. 20). Lo referido a la privacidad en las comunicaciones se reconoce de manera separada y se incluye a todo tipo de comunicación física o virtual:

> «El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación» (art. 66.21).

El Código Orgánico Integral Penal (COIP) regula la posibilidad de intervención en las comunicaciones mediante la llamada «interceptación de las comunicaciones o datos informáticos» (art. 476); esto debe ser autorizado por un juez a solicitud fundamentada de un fiscal, cuando existan indicios que resulten relevantes a los fines de la investigación, de conformidad con las siguientes reglas: es el juez quien determina la comunicación interceptada y el tiempo de intercepción, tiempo que no podrá ser mayor a un plazo de noventa días, cuando este plazo se cumpla, se podrá solicitar, motivadamente, una prórroga hasta por un plazo de noventa días más; en los casos de investigaciones de delincuencia organizada y sus delitos relacionados, la interceptación podrá realizarse hasta por un plazo de seis meses y se podrá solicitar motivadamente la ampliación por igual período de tiempo.

En caso de obtenerse información relacionada con la infracción durante la interceptación, esta puede ser utilizada únicamente en el proceso para el cual fue autorizada la interceptación. Existe la obligación de guardar secreto respecto de los asuntos ajenos al hecho que motivó su examen; en caso de llegar a conocimiento de las autoridades la comisión de otra infracción, esto debe comunicarse inmediatamente al fiscal, para que se dé inicio a una investigación, con excepción de delitos flagrantes.

La interceptación y el registro de datos informáticos pueden hacerse en los servicios de telecomunicaciones como telefonía fija, satelital, móvil e inalámbrica, se incluyen los servicios de llamadas de voz, mensajes SMS, mensajes MMS, transmisión de datos y voz sobre IP, correo electrónico, redes sociales, videoconferencias y multimedia.

Se establecen dos prohibiciones de forma expresa a las interceptaciones: i) la primera tiene que ver con aquellas comunicaciones protegidas por el secreto profesional o religioso y la interceptación, grabación y transcripción de comunicaciones que vulneren los derechos de los niños, niñas y adolescentes, especialmente en aquellos casos que generen la revictimización por infracciones de violencia contra la mujer o miembros del núcleo familiar; la violencia puede ser de tipo sexual, física, sicológica, etc. Los fiscales son los funcionarios autorizados para conservar la información obtenida en la interceptación.

4.7. Derecho a la imagen

En el CNA el derecho a la imagen se encuentra ligado a los derechos a la libertad y dignidad, el artículo 51 -que lo contiene- se titula «Derecho a la libertad personal, dignidad, reputación, honor e imagen» y al desarrollarse se lo trata como derecho a la «dignidad, autoestima, honra, reputación e imagen propia», un interesante enfoque que sitúa al derecho como parte del derecho a libertad protegido en función de la dignidad, autoestima, honra y reputación.

En la Constitución, el derecho a la imagen se encuentra reconocido como parte del derecho al honor y al buen nombre: «El derecho al honor y al buen nombre. La ley protegerá la imagen y la voz de la persona» (art. 66. 18)

En el CNA (art. 52) se establecen algunas prohibiciones a la utilización de la imagen de las personas menores de edad en programas, mensajes publicitarios, producciones de contenido pornográfico y espectáculos cuyos contenidos sean inadecuados para su edad, también en programas o espectáculos de proselitismo político o religioso, publicación o exhibición de noticias, reportajes, crónicas, historias de vida o cualquiera otra expresión periodística con imágenes o nombres propios de niños, niñas o adolescentes que han sido víctimas de maltrato o abuso, publicación o exhibición de imágenes y grabaciones o referencias escritas que permitan la identificación o individualización de un niño, niña o adolescente que ha sido víctima de maltrato, abuso sexual o infracción penal y cualquier otra referencia al entorno en el que se desarrollan; además, se prohíbe la publicación del nombre, así como la imagen de los menores acusados o sentenciados por delitos o faltas. La infracción a estas prohibiciones puede configurar un delito, como se examinará más adelante, además de la sanción de multa que el CNA prevé para estos casos[30].

En el artículo 52 del CNA también se regula el uso autorizado de las imágenes de los menores de edad, diferenciándose la situación de niños y niñas y de los adoles-

30 Art. 251.- Infracciones contra el derecho a la intimidad y a la imagen.- Serán sancionados con la multa señalada en el artículo 248:

1. Los medios de comunicación, los responsables de su programación o edición y los periodistas que difundan informaciones que permitan o posibiliten la identificación de un adolescente involucrado en un enjuiciamiento penal o de sus familiares;

2. Los medios y personas señalados en el numeral anterior, que publiquen o exhiban reportajes, voz o imagen o cualquier dato o información que permita identificar a un niño, niña o adolescente que ha sido objeto de cualquiera forma de maltrato o abuso sexual;

3. Los funcionarios públicos que por cualquier medio, directa o indirectamente, hagan o permitan que se hagan públicos los antecedentes policiales o judiciales de los adolescentes que hayan sido investigados, enjuiciados o privados de su libertad con motivo de una infracción penal, en contravención de lo dispuesto por el artículo 53;

4. Los que utilicen la imagen de un niño, niña o adolescente en cualquier medio de comunicación o recurso publicitario sin la autorización expresa de este último o de su representante legal; y,

5. Las personas naturales o jurídicas que distorsionen, ridiculicen o exploten a través de cualquier medio la imagen de los niños, niñas o adolescentes con discapacidad.».

centes mayores de 15 años. En el primer caso, es posible la utilización pública de su imagen con la autorización del representante legal[31]; en el segundo, el uso debe ser autorizado de forma expresa por el adolescente. En los dos casos debe tratarse de usos no prohibidos.

Las prohibiciones al uso de la imagen dispuestas en el CNA son recogidas en el COIP, en la Ley Orgánica de Comunicación (LOC) y en la Ley Orgánica de Telecomunicaciones (LOT).

4.8. Integridad personal

El derecho a la integridad personal está ampliamente reconocido en la legislación nacional. El CNA, en la parte pertinente del artículo 50, establece que los NNA «(…) tienen derecho a que se respete su integridad personal, física, psicológica, cultural, afectiva y sexual(…)». Se proscribe toda forma de maltrato, al que se lo define (art. 67) como

> «(…)toda conducta, de acción u omisión, que provoque o pueda provocar daño a la integridad o salud física, psicológica o sexual de un niño, niña o adolescente, por parte de cualquier persona, incluidos sus progenitores, otros parientes, educadores y personas a cargo de su cuidado; cualesquiera sean el medio utilizado para el efecto, sus consecuencias y el tiempo necesario para la recuperación de la víctima(…)».

El maltrato puede ser de cuatro clases: psicológico, abuso sexual, institucional y físico. Como se verá más adelante, al revisar sus definiciones, las tres primeras clases de maltrato pueden tener como escenario las TIC's.

Ocasionar «(…) perturbación emocional, alteración psicológica o disminución de la autoestima en el niño, niña o adolescente agredido» y también se incluyen «(…) las amenazas de causar un daño en su persona o bienes de sus progenitores, otros parientes o personas encargadas de su cuidado», todo esto es considerado maltrato sicológico.

Abuso sexual (art. 68) es, para la aplicación de las medidas de protección del CNA, «(…) todo contacto físico, sugerencia de naturaleza sexual, a los que se somete un niño, niña o adolescente, aun con su aparente consentimiento, mediante seducción, chantaje, intimidación, engaños, amenazas, o cualquier otro medio».

El maltrato es considerado institucional cuando puede atribuirse al servidor de una institución pública o privada y es resultado de la aplicación de reglamentos, prácticas administrativas o pedagógicas aceptadas expresa o tácitamente por la institución y cuando sus autoridades lo han conocido y no han adoptado las medidas para prevenirlo, hacerlo cesar, remediarlo y sancionarlo de manera inmediata.

31En aplicación de las reglas generales sobre consulta a niños, niñas y adolescentes esta decisión únicamente debería otorgarse contado con la opinión de los menores de edad involucrados.

La responsabilidad por maltrato institucional recae en el autor del maltrato y en el representante legal, autoridad o responsable de la institución o establecimiento al que pertenece.

Sujetos activos de maltrato pueden ser los adultos o sus iguales. En el texto de la norma se establece con claridad que podría ser ocasionado por cualquier persona, incluidos sus progenitores, otros parientes, educadores y personas a cargo de su cuidado, es decir, no exclusivamente ellos; esto es importante porque podría permitir enfrentar ciertas prácticas de acoso en línea que no se configuran alguna forma de violencia intrafamiliar u otro delito.

4.9. Derecho a la recreación y al juego

En el artículo 80 del CNA se reconoce el derecho de los NNA a la recreación, al descanso, al juego, al deporte y más actividades propias de cada etapa evolutiva; si bien se da prioridad a los juegos tradicionales y a las actividades artísticas, deportivas y culturales, el Consejo de Regulación de Desarrollo de la Información y la Comunicación tiene la competencia de establecer la regulación para el "uso de juegos y programas computarizados y electrónicos"[32].

En la Constitución, este derecho aparece en el artículo 66.2 como parte del derecho a la vida digna (descanso y ocio) y en las reglas específicas de niñez y adolescencia en cuanto al deporte y la recreación (art. 45). Una regla que podría aplicarse a internet se encuentra en el artículo 46.7 que considera obligación del Estado proteger a los NNA de

> "(…) la influencia de programas o mensajes, difundidos a través de cualquier medio, que promuevan la violencia, o la discriminación racial o de género. Las políticas públicas de comunicación priorizarán su educación y el respeto a sus derechos de imagen, integridad y los demás específicos de su edad".

En las normas citadas no existe referencia al internet, juegos en línea o similares, pero estas pueden usarse para restringir el acceso a internet por parte de menores de edad.

4.10. Normas penales

El Código Orgánico Integral Penal del año 2014 tiene un número importante de tipos penales aplicables o relacionados con conductas que pueden expresarse en internet; además, ciertas reglas relacionadas a la aplicación territorial de las normas penales facilitarían la persecución de los delitos que se comenten por medio de las TIC's. En cuanto al ámbito espacial de aplicación, (art. 14) es posible perseguir ciertas conductas tipificadas en legislación penal ecuatoriana, cuando estas

32 Registro Oficial Suplemento 283 de 7 de julio de 2014.

son cometidas fuera del territorio, en los siguientes casos: a) cuando la infracción produzca efectos en el Ecuador o en los lugares sometidos a su jurisdicción; b) cuando la infracción penal es cometida en el extranjero, contra una o varias personas ecuatorianas y no ha sido juzgada en el país donde se la cometió.

No pueden negarse las dificultades prácticas de la aplicación de esta regla de extraterritorialidad, sin embargo, esta misma regla abre la puerta para la persecución de ciertas conductas que por su naturaleza pueden cometerse fuera del territorio ecuatoriano.

Algunos de los delitos relacionados con las TIC's o que pueden perpetrarse por medio de ellas consideran de forma específica la cuestión de la edad; sin embargo, debe recordarse que la edad es una circunstancia agravante -general- de toda infracción penal que se cometa en perjuicio de niñas, niños, adolescentes o que se valga de ellos para la comisión de la infracción (art. 47 números 10 y 11 COIP).

Para las infracciones contra la integridad sexual y reproductiva, la integridad y la libertad personal (art. 48 COIP) se consideran como agravantes específicas: que la víctima, al momento de la infracción, se encuentre al cuidado o recibiendo atención en establecimientos públicos o privados, tales como los de salud, educación u otros similares; el compartir el núcleo familiar con la víctima; y, tener el sujeto activo del delito algún tipo de relación de poder o autoridad sobre la víctima, puede ser un funcionaria o funcionario público, docente, ministras o ministros de algún culto, funcionarios o funcionarias de la salud o personas responsables en la atención del cuidado del paciente; se incluye cualquier otra clase de profesional o persona que haya abusado de su posición, función o cargo para cometer la infracción.

En los delitos de la sección trata de personas y diversas formas de explotación (art. 110) existen una serie de disposiciones relevantes aplicables a niños, niñas y adolescentes: de forma adicional a la pena privativa de libertad pueden imponerse una o varias penas no privativas de libertad; en los casos en los que la o el presunto agresor sea ascendiente o descendiente o colateral hasta el cuarto grado de consanguinidad o segundo de afinidad, cónyuge, ex cónyuge, conviviente, ex conviviente, pareja o ex pareja en unión de hecho, tutora o tutor, representante legal, curadora o curador o cualquier persona a cargo del cuidado o custodia de la víctima, el juez de Garantías Penales como medida cautelar suspenderá la patria potestad, tutoría, curatela y cualquier otra modalidad de cuidado sobre la víctima, a fin de proteger sus derechos; el comportamiento público o privado de la víctima, anterior a la comisión de la infracción sexual, no es considerado dentro del proceso; en estos delitos, el consentimiento dado por la víctima menor de dieciocho años de edad es irrelevante.

En los delitos contra la integridad sexual y reproductiva se reproducen las mismas consideraciones citadas en el párrafo anterior (art. 175).

La relevancia de estas disposiciones para el caso de las TIC's son indiscutibles, no importa el uso que la víctima haya hecho de las redes sociales o de las tecnologías de información, no tiene relevancia legal que la víctima se haya expuesto al riesgo de alguna forma o que haya expresado alguna forma de consentimiento. La desaparición del error de prohibición del proyecto del COIP deja abierta la persecución en aquellos casos en que el sujeto activo de la infracción afirme que no tenía conocimiento que la víctima era menor de edad. Esto podría tener un impacto en aquellos casos en los que la niña, el niño o el adolescente han asumido otra identidad en la red.

4.10.1 Tipos penales específicos relacionados a las TIC's y que consideran como sujetos pasivos específicos a menores de edad.

Cuatro tipos penales consideran el uso de las TIC's y tienen como sujetos pasivos específicos del delito a personas menores de 18 años de edad. Dos sancionan formas de explotación (utilización, posesión y comercialización de pornografía con menores de 18 años), dos la vulneración a la libertad sexual (contacto con finalidad sexual con menores de 18 años y oferta de servicios sexuales con menores de 18 años por medios electrónicos).

Formas de explotación

Se sanciona la utilización de niños, niñas y adolescentes en pornografía. El tipo penal (art. 103) sanciona a la persona que

> « (…) fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual»,

Este delito se sanciona con una pena privativa de libertad de trece a dieciséis años. En caso de que, además, la víctima sufra algún tipo de discapacidad o enfermedad grave o incurable, la sanción será de dieciséis a diecinueve años de privación de la libertad. Cuando la persona infractora sea el padre, la madre, pariente hasta el cuarto grado de consanguinidad o segundo de afinidad, tutor, representante legal, curador o pertenezca al entorno íntimo de la familia; ministro de culto, profesor, maestro, o persona que por su profesión o actividad haya abusado de la víctima, la sanción será la pena privativa de libertad de veintidós a veintiséis años.

La posesión para uso personal o el intercambio de pornografía en la se utilice a menores de 18 años se sanciona con pena privativa de la libertad de 10 a 13 años (art. 104). En esta conducta se incluye a quien «publicite, compre, posea, porte, transmita, descargue, almacene, importe, exporte o venda, por cualquier medio» pornografía de niños, niñas y adolescentes.

Vulneración a la libertad sexual

Para esta clase de delitos se consideran dos tipos penales:

El primero es el contacto con finalidad sexual con menores de dieciocho años por medios electrónicos (art. 173). Se sanciona con una pena de uno a tres años de privación de la libertad, a la persona que « (…) a través de un medio electrónico o telemático proponga concertar un encuentro con una persona menor de dieciocho años, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento con finalidad sexual o erótica». Cuando el acercamiento se obtiene mediante coacción o intimidación, la persona deberá ser sancionada con una pena privativa de libertad de tres a cinco años. En caso de que para cometer este delito se hubiese suplantando la identidad de un tercero o se haya usado una identidad falsa para, por medios electrónicos o telemáticos, establecer comunicaciones de contenido sexual o erótico con una persona menor de dieciocho años o con discapacidad, el responsable será sancionado con pena privativa de libertad de tres a cinco años. El segundo tipo penal, es la oferta de servicios sexuales, por medios electrónicos, de menores de 18 años se sanciona con pena de 7 a 10 años. Este tipo penal sanciona a la persona que « (…) utilice o facilite el correo electrónico, chat, mensajería instantánea, redes sociales, blogs, fotoblogs, juegos en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexuales…».

4.10.2 Tipos penales específicos relacionados a las TIC's y que no consideran como sujeto pasivo específico a los menores de 18 años

Seis delitos se pueden identificar bajo esta categoría. Cuatro se dirigen a proteger la vida privada, intimidad o integridad de la información (violación a la intimidad; intercambio, comercialización o compra de información de equipos terminales móviles; revelación ilegal de bases de datos e interceptación ilegal de datos); dos protegen el derecho de propiedad (apropiación fraudulenta por medios electrónicos y transferencia electrónica de activo patrimonial).

Delitos que violan la vida privada, intimidad o integridad de la información

El delito de violación a la intimidad

El artículo 178 tipifica como delito de violación a la intimidad a quien

> «(…) sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio(…)».

Esa conducta se sanciona con pena privativa de libertad de uno a tres años. No son aplicables estas normas a la persona que divulgue grabaciones de audio y

vídeo en las que interviene personalmente ni cuando se trata de información pública, de acuerdo con lo previsto en la ley.

Este tipo penal parecería no aplicable a progenitores o maestros que accedan, intercepten o examinen los mensajes de datos, voz, audio y vídeo, por la disposición del artículo 53 del CNA que, al reconocer el derecho a la privacidad, la inviolabilidad del hogar y las formas de comunicación, incluye una noción de «natural vigilancia de los padres y maestros» que no se corresponde con las normas internacionales en la materia que no hablan de «vigilancia» sino de «guía en el ejercicio de los derechos». Sin embargo, una lectura compatible con los derechos impide considerar esta regla como una suerte de cheque en blanco que autorizaría cualquier intervención. Para justificar debe cumplirse el test de necesidad y proporcionalidad, además de considerar la edad y madurez del menor de edad, ya que no justificar esa intervención podría considerarse como una injerencia arbitraria o ilegal en su vida privada. En cuanto a los maestros, la posibilidad de intervención me parece mucha más reducida que la de los progenitores y únicamente podría alegarse que se hace en protección de su interés superior, pero esto exige una demostración de un daño concreto no potencial o imaginado. La difusión o publicación de información que no tenga por objeto cierto la protección de su interés superior[33] debería ser sancionada como delito.

En el artículo 192 se prevé una sanción penal de uno a tres años a quien «(…) intercambie, comercialice o compre bases de datos que contengan información de identificación de equipos terminales móviles(…)».

En el artículo 229 se castiga la revelación ilegal de bases de datos cuando una persona

> «(…) en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas(…)».

Esta conducta se sanciona con pena privativa de libertad de uno a tres años. Si la conducta se comete por un servidor público, empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, la pena será de tres a cinco años.

33En esta materia, la apreciación del interés superior del Niño son relevantes la Observación General No. 14 del CRC de… y en el ámbito Interamericano la sentencia del caso Átala Riffo c. Chile, en los dos instrumentos se establece con claridad la necesidad de establecer de forma cierta cuál es la amenaza o el beneficio para el interés superior del niño de cualquier medida concreta o general que se tome, es decir, no son suficientes consideraciones de carácter general o especulativas respecto del ventanal beneficio o la amenaza invocada.

La interceptación ilegal de datos es sancionada, en el artículo 230, con una pena de tres a cinco años cuando: sin orden judicial previa, en provecho propio o de un tercero, se intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales, con la finalidad de obtener información registrada o disponible; quien diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o quien modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder; al que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico, información que esté soportada en las tarjetas de crédito, débito, pago o similares; a la persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito anterior.

El artículo 231 castiga la transferencia electrónica de activo patrimonial, este delito se configura cuando una persona

> «(…) con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona».

En el artículo 232 se considera como delito de ataque a la integridad de sistemas informáticos el que una persona

> «(…) destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen; de igual forma se sanciona a quien diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados; y, a quien destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general».
>
> En todos estos supuestos, la pena privativa de la libertad es tres a cinco años.

4.10.3 Tipos penales que pueden aplicarse a conductas que se den en las TIC's sin mención específica a estas.

Existen otros delitos que podrían aplicarse a conductas en las que los menores de 18 años son víctimas y que podrían perpetrarse por medio de las las TIC's, pero no se las menciona de forma específica, es importante. Algunos de esos tipos penales permiten encarar conductas consideradas especialmente intolerables como la amenaza e intimidación (art. 154[34]), los actos de oído (art. 177[35]), la suplantación de identidad (art. 212[36]), la violencia sicológica[37] (art. 157[38]), la corrupción de NNA

---

34 "Intimidación.- La persona que amenace o intimide a otra con causar un daño que constituya delito a ella, a su familia, a personas con las que esté íntimamente vinculada, siempre que, por antecedentes aparezca verosímil la consumación del hecho, será sancionada con pena privativa de libertad de uno a tres años".

35 "Actos de odio.- La persona que cometa actos de violencia física o psicológica de odio, contra una o más personas en razón de su nacionalidad, etnia, lugar de nacimiento, edad, sexo, identidad de género u orientación sexual, identidad cultural, estado civil, idioma, religión, ideología, condición socioeconómica, condición migratoria, discapacidad, estado de salud o portar VIH, será sancionada con pena privativa de libertad de uno a tres años. Si los actos de violencia provocan heridas a la persona, se sancionará con las penas privativas de libertad previstas para el delito de lesiones agravadas en un tercio. Si los actos de violencia producen la muerte de una persona, será sancionada con pena privativa de libertad de veintidós a veintiséis años".

36 "Suplantación de identidad.- La persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, será sancionada con pena privativa de libertad de uno a tres años".

37 Este delito únicamente podría aplicarse en los casos que el sujeto activo es miembro del núcleo familiar de la víctima, de acuerdo a la definición contenida en el segundo párrafo del art. 155 del COIP "Se consideran miembros del núcleo familiar a la o al cónyuge, a la pareja en unión de hecho o unión libre, conviviente, ascendientes, descendientes, hermanas, hermanos, parientes hasta el segundo grado de afinidad y personas con las que se determine que el procesado o la procesada mantenga o haya mantenido vínculos familiares, íntimos, afectivos, conyugales, de convivencia, noviazgo o de cohabitar

38 "Violencia psicológica contra la mujer o miembros del núcleo familiar.- La persona que, como manifestación de violencia contra la mujer o miembros del núcleo familiar, cause perjuicio en la salud mental por actos de perturbación, amenaza, manipulación, chantaje, humillación, aislamiento, vigilancia, hostigamiento o control de creencias, decisiones o acciones, será sancionada de la siguiente manera:

1. Si se provoca daño leve que afecte cualquiera de las dimensiones del funcionamiento integral de la persona, en los ámbitos cognoscitivos, afectivos, somáticos, de comportamiento y de relaciones, sin que causen impedimento en el desempeño de sus actividades cotidianas, será sancionada con pena privativa de libertad de treinta a sesenta días.
2. Si se afecta de manera moderada en cualquiera de las áreas de funcionamiento personal, laboral, escolar, familiar o social que cause perjuicio en el cumplimiento de sus actividades cotidianas y que por tanto requiere de tratamiento especializado en salud mental, será sancionada con pena de seis meses a un año.
3. Si causa un daño psicológico severo que aún con la intervención especializada no se ha logrado revertir, será sancionada con pena privativa de libertad de uno a tres años".

(art. 169[39]), la distribución de material pornográfico (art. 168[40]) o la captación por medios electrónicos para trata de personas (art. 91[41]). También podrían incluirse delitos como la difusión de información restringida de menores de edad (art. 180[42]), la calumnia (art. 182[43]), la violación a la intimidad (art. 178[44]) y el impedi-

39 "Corrupción de niñas, niños y adolescentes.- La persona que incite, conduzca o permita la entrada de niñas, niños o adolescentes a prostíbulos o lugares en los que se exhibe pornografía, será sancionada con pena privativa de libertad de tres a cinco años".

40 "Distribución de material pornográfico a niñas, niños y adolescentes.- La persona que difunda, venda o entregue a niñas, niños o adolescentes, material pornográfico, será sancionada con pena privativa de libertad de uno a tres años".

41 "Trata de personas.- La captación, transportación, traslado, entrega, acogida o recepción para sí o para un tercero, de una o más personas, ya sea dentro del país o desde o hacia otros países con fines de explotación, constituye delito de trata de personas.

Constituye explotación, toda actividad de la que resulte un provecho material o económico, una ventaja inmaterial o cualquier otro beneficio, para sí o para un tercero, mediante el sometimiento de una persona o la imposición de condiciones de vida o de trabajo, obtenidos de:

1. La extracción o comercialización ilegal de órganos, tejidos, fluidos o material genético de personas vivas, incluido el turismo para la donación o trasplante de órganos.
2. La explotación sexual de personas incluida la prostitución forzada, el turismo sexual y la pornografía infantil.
3. La explotación laboral, incluida el trabajo forzoso, la servidumbre por deudas y el trabajo infantil.
4. Promesa de matrimonio o unión de hecho servil, incluida la unión de hecho precoz, arreglada, como indemnización o transacción, temporal o para fines de procreación.
5. La adopción ilegal de niñas, niños y adolescentes.
6. La mendicidad.
7. Reclutamiento forzoso para conflictos armados o para el cometimiento de actos penados por la ley.
8. Cualquier otra modalidad de explotación".

42 "Difusión de información de circulación restringida.- La persona que difunda información de circulación restringida será sancionada con pena privativa de libertad de uno a tres años.

Es información de circulación restringida:

1. La información que está protegida expresamente con una cláusula de reserva previamente prevista en la ley.
2. La información producida por la Fiscalía en el marco de una investigación previa.
3. La información acerca de las niñas, niños y adolescentes que viole sus derechos según lo previsto en el Código Orgánico de la Niñez y Adolescencia".

43 "Calumnia.- La persona que, por cualquier medio, realice una falsa imputación de un delito en contra de otra, será sancionada con pena privativa de libertad de seis meses a dos años.
No constituyen calumnia los pronunciamientos vertidos ante autoridades, jueces y tribunales, cuando las imputaciones se hubieren hecho en razón de la defensa de la causa.
No será responsable de calumnias quien probare la veracidad de las imputaciones. Sin embargo, en ningún caso se admitirá prueba sobre la imputación de un delito que hubiere sido objeto de una sentencia ratificatoria de la inocencia del procesado, de sobreseimiento o archivo.
No habrá lugar a responsabilidad penal si el autor de calumnias, se retractare voluntariamente antes de proferirse sentencia ejecutoriada, siempre que la publicación de la retractación se haga a costa del responsable, se cumpla en el mismo medio y con las mismas características en que se difundió la imputación. La retractación no constituye una forma de aceptación de culpabilidad".

44 "Violación a la intimidad.- La persona que, sin contar con el consentimiento o la autorización

mento del ejercicio la libertad de expresión (art. 183[45]).

4.11. Adolescentes como sujetos activos de violaciones a derechos de terceros

La regla general en esta materia es que los niños y niñas (personas menores de 12 años) son inimputables e irresponsables penalmente, por tanto, en caso realizar una de las conductas descritas como tipos penales, no serán juzgados y las autoridades deberán tomar medidas de protección, que podría incluir acciones dirigidas contra sus progenitores o responsables, cuando sus acciones sean producto de la omisión de sus obligaciones de cuidado y crianza, lo que contemplaría las acciones civiles derivadas del daño causado por la conducta del niño o niña (art. 307 CNA).

Los adolescentes son inimputables, pero responsables penalmente (art. 305 CNA), son sujetos de responsabilidad penal cuando comenten infracciones tipificadas en el COIP (art. 306 CNA).

En cuanto a las posibles violaciones a los derechos de propiedad intelectual de terceros, es posible aplicar la legislación general en la materia; sin embargo, existen particularidades en el tema de la responsabilidad civil generada por las posibles infracciones, ya que en ciertas circunstancias los responsables de esos daños serían quienes los tienen bajo su cuidado[46]. Este es un tema complejo que requiere de un análisis más detallado que supera los objetivos del presente trabajo.

5. Conclusiones provisorias

Existe algún consenso sobre las líneas principales de las políticas públicas y normativas en la relación entre internet y niños, niñas y adolescentes, algunas de estas recomendaciones son asimilables al contexto ecuatoriano:

- Es necesario un enfoque positivo sobre derechos humanos, cualquier política pública o regulación debe partir del reconocimiento de niños, niñas y ado-

legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley".

45 "Restricción a la libertad de expresión.- La persona que, por medios violentos, coarte el derecho a la libertad de expresión, será sancionada con pena privativa de libertad de seis meses a dos años".

46 Art. 2219 del CC "No son capaces de delito o cuasidelito los menores de siete años, ni los dementes; pero serán responsables de los daños causados por ellos las personas a cuyo cargo estén, si pudiere imputárseles negligencia.
Queda a la prudencia del juez determinar si el menor de diez y seis años ha cometido el delito o cuasidelito sin discernimiento; y en este caso se seguirá la regla del inciso anterior".

lescentes como sujetos plenos de derechos y, por tanto, la potencialidad que tienen para el ejercicio de sus derechos, que tengan acceso al internet y que comprendan las graves consecuencias que tiene la exclusión, la misma que podría tener un impacto negativo en la vida y desarrollo de NNA.

- Las necesidades de protección a la infancia y adolescencia en ningún caso pueden satisfacerse restringiendo su acceso a las TIC's; en esta materia, es de especial relevancia la educación, particularmente a los adolescentes[47] y reconocer el rol que tienen los pares en el fomento del uso de la tecnología y el desarrollo de hábitos y prácticas de protección y uso seguro[48]. Los adultos sobredimensionan las amenazas en la red[49], estas pueden crecer si no se enfrentan, pero nunca a costa del acceso o la censura.

- El marco jurídico ecuatoriano que regula de forma específica el acceso y uso al internet por parte de los menores de edad es limitado, sin embargo, es posible identificar una cantidad importante de disposiciones aplicables que reconocen el derecho al acceso y que establecen las responsabilidades para la prevención, investigación y sanción a la vulneración de derechos en línea, teniendo a NNA como víctimas o victimarios.

- Algunas limitaciones a los derechos contenidos en el CNA, por ejemplo, el derecho a la vida privada, da un poder excesivo a padres y maestros para intervenir en las comunicaciones personales, sin necesidad de justificación alguna, por esto, deben leerse estas reglas en el contexto de las normas de protección de derechos, esto implica que la restricción únicamente podría darse cuando se justifique la necesidad de la misma. En el caso de los maestros, esta opción es más limitada aún y debería entenderse como excepcional.

- Existe un vacío sobre el acoso en línea entre iguales, sin embargo, las normas sobre maltrato del CNA y las disposiciones referidas a los delitos contra la mujer o miembros del núcleo familiar y discriminación, particularmente el sicológico, pueden ser aplicadas para enfrentar estas conductas, tanto en el ámbito de la prevención, como en el de la protección y sanción. Sin embargo, parecería necesario contar con un tipo penal específico que castigue el acoso en línea.

- Un elemento relevante a considerar en esta materia es la obligación del Estado de perseguir las conductas violatorias a los derechos que se den en el internet, particularmente en aquellos casos en los que estas conductas sean

---

47 En este enfoque coinciden el CRC, el documento de María Isabel Pavez publicado por la CEPAL y los trabajos de Livingston

48 CRC, el documento de María Isabel Pavez publicado por la CEPAL y los trabajos de Livingston

49 *Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres,* Observatorio de la Seguridad de la Información, marzo, 2009, pág. 13.

delitos. La persecución a los infractores y a los abusivos es central, es necesario dar efectividad a las reglas que sancionan los comportamientos abusivos en la red e impedir la impunidad. Hay varias dificultades por la llamada deslocalización de los delitos que se producen en el escenario virtual, sin embargo, existen los mecanismos normativos para esta persecución, pero, especialmente, se requiere de cooperación internacional para enfrentar estas conductas.

- Una medida importante es la de fomentar los espacios de acceso seguro a las TIC's y reconocer el peligro que representan los cibercafés o similares y, por tanto, la necesidad de tomar acciones para que estos se conviertan en espacios seguros.

- Es necesario trabajar para contar con evidencia empírica y debidamente contextualizada sobre el uso de internet por parte de niños, niñas y adolescentes; la información disponible en el Ecuador es limitada e insuficiente para la generación de políticas públicas y respuestas normativas adecuadas[50].

Bibliografía:

Bringué, Sábada y Tolsá, "La Generación Interactiva en Iberoamérica 2010. Niños y adolescentes ante las pantallas", Colección Generaciones Interactivas-Fundación Telefónica, Madrid, 2011.

Committee on the Rights of the Children, Report of the 2014 Day of General Discussion «Digital media and children's rights, Geneva, 2014, disponible en línea http://www.ohchr.org/Documents/HRBodies/CRC/Discussions/2014/DGD_report.pdf.

Corte Constitucional Colombiana, sentencia T-260/12, disponible en http://www.corteconstitucional.gov.co/relatoria/2012/T-260-12.HTM.

Corte Interamericana de Derechos Humanos, El Derecho a la Información sobre la Asistencia Consular en el Marco de las Garantías del Debido Proceso Legal, Opinión Consultiva OC-16/99 de 1 de octubre de 1999, Serie A, No. 16.

Gasser, Urs, et. all.,Working Towards a Deeper Understanding of Digital Safety for Children and Young People in Developing Nations, Berkman Center for Internet & Society at Harvard University, in Collaboration with UNICEF, 2010.

Guallpa, L., Vulneración de derechos de niñ@s y adolescentes por el uso patológico de redes sociales digitales" presentado en el III Congreso Científico In-

---

50 Un ejemplo del tipo de información empírica que debería contarse en el país puede encontrarse en el estudio de Livingstone y Haddon citado en este estudio; en la investigación de Bringué, Sábada y Tolsá, la Generación Interactiva en Iberoamérica 2010, disponible en línea en http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0122-82852012000300018.

ternacional Uniandes: Impacto de las investigaciones universitarias, de 30 de julio de 2015, disponible en http://www.uniandes.edu.ec/web/wp-content/uploads/2016/04/Vulneración-de-derechos-de-niñ@s-y-adolescentes-por-el-uso-patológico-.pdf.

Redes sociales digitales y derechos de la niñez y adolescencia en Ecuador, publicado en Episteme, Revista de Ciencia y Tecnología e Innovación, Volumen 1, número 2 (2014), disponible en http://186.46.158.26/ojs/index.php/EPISTEME/article/view/32).

Redes sociales digitales y derechos de la niñez y adolescencia en Ecuador, publicado en Episteme, Revista de Ciencia y Tecnología e Innovación, Volumen 1, número 2 (2014), disponible en http://186.46.158.26/ojs/index.php/EPISTEME/article/view/32).

Internet Society, "Internet y los niños", s/f, www.bp-childrenandtheinternet-20129017-en_ES.

Lansdown, G., La evolución de las facultades del niño. UNICEF-Save the Children: Centro de Investigaciones Innocenti. Florencia-Italia. s/f.

Livingstone, S., y Haddon, L., EU Kids Online: Final report, 2009, London School Of Economics and Political Science, 2009, LSE, London: EU Kids Online.

Observatorio Social del Ecuador, Niñez y Adolescencia desde la Intergeneracionalidad, UNICEF, CNII, Save the Children, Plan Internacional, Quito, 2015, p. 113. Disponible en línea http://www.unicef.org/ecuador Ninez_Adolescencia_Intergeneracionalidad_Ecuador_2016_WEB2.pdf.

Pavez, M. I., Los derechos de la infancia en la era de Internet: América Latina y las nuevas tecnologías, Cepal-Unicef, Cepal, Serie Políticas Sociales No. 210, Santiago, 2014.

Ramón Fernández, F., Menores y Redes Sociales, cuestiones legales, publicado en Revista sobre la Infancia y Adolescencia, No. 8, abril 2015.

Revelo Herrera, H., Trujillo, M. Cibercrimen y de los Derechos de los niños, jóvenes adolescentes y jóvenes adultos. Este artículo se encuentra disponible en http://oiprodat.com/2014/05/01/proteccion-a-ninos-jovenes-adolescentes-y-jovenes-adultos-en-internet-medios-electronicos-y-redes-sociales/.

http://oiprodat.com/2014/05/01/proteccion-a-ninos-jovenes-adolescentes-y-jovenes-adultos-en-internet-medios-electronicos-y-redes-sociales/.

Simon, F. El enfoque de derechos en el "Memorándum de Montevideo", publicado en Protección de datos personales en las redes sociales digitales: en particular de niños y adolescentes. Memorándum de Montevideo, compiladores Carlos G. Gregorio y Lina Ornelas, IFAI, México D.F., 2011.

Third, A. et. al, Children's Rights in the Digital Age: A download from children around the world, Second edition, Young and Well Cooperative Research Centre, Melbourne, 2014.

Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2015.

Unión Europea, Directiva del Parlamento Europeo y del Consejo relativo a la lucha contra los abusos sexuales, la explotación sexual de los niños y La pornografía infantil, por la que se deroga la Decisión marco 2004/68/JAI, Unión Europea, Bruselas, 4 de noviembre de 2011.

UNICEF, Centro de Investigaciones Innocenti, La seguridad de los niños en línea: retos y estrategias mundiales, Florencia, 2012.

Memorandum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes, "Memorando de Montevideo", Montevideo, 28 de julio de 2009. Disponible en http://clicseguro.sep.gob.mx/archivos/Memorandum_Montevideo.pdf.

Telecomunicaciones e internet en el Ecuador del Siglo XXI: Apuntes técnicos, historia reciente y la ruta hacia el control de usuarios y contenidos

Juan Carlos Solines Moreno
Solines & Asociados

RESUMEN: La penetración global de la telefonía móvil y las tecnologías inalámbricas emergentes alteraron de manera dramática la industria de telecomunicaciones. Internet se ha convertido en uno de los más importantes recursos para los gobiernos y el sector privado, así como también en una herramienta básica para la sociedad. La ley y la regulación es aplicable a países y jurisdicciones específicas, pero la arquitectura de Internet y sus recursos críticos tienen implicaciones que van más allá de lo local. Ecuador inició un proceso de apertura y liberalización de las telecomunicaciones que dio paso a un crecimiento exponencial de estos servicios incluido Internet y el número de usuarios de esos servicios. Sin embargo, dentro del proceso de empoderamiento de la sociedad, con un crecimiento de los flujos de información y una notoria influencia de las redes sociales, el Estado ecuatoriano evidencia una estrategia de regulación, un modelo de diseño institucional y ciertas políticas públicas que se orientarían al control de usuarios y contenidos.

Incluso aspectos técnicos tales como la asignación y administración del espectro y principios como el de neutralidad de la red están bajo riesgo de influencia política, la misma que puede afectar adversamente a los derechos fundamentales y al desarrollo de la Sociedad de la Información en Ecuador.

PALABRAS CLAVE: Internet, telecomunicaciones, Ecuador, ciberespacio, regulación, censura, control.

ABSTRACT: The global penetration of mobile telephony and the emergence of wireless technologies dramatically altered the Telecommunications industry. Internet has become one of the most important resources for governments and private sector, as well as a basic tool for society. Law and regulation apply to specific countries and jurisdictions, but the architecture of Internet and its critical resources have implications that go beyond local. Ecuador started to open and liberalize its telecom industry, bringing an exponential growth of telecom services, including Internet, and users. However, within the process of social empowerment with a substantial growth of information flows and a notorious influence of social networks, the State reveals a regulation strategy, a model of institutional design and some policies aimed to gain control over users and content. Even technical aspects such as spectrum allocation and management and principles like net neutrality are under risk of political influence that may adversely affect fundamental rights and the development of the Information Society in Ecuador.

KEYWORDS: Internet, telecommunications, Ecuador, cyberspace, regulation, censorship, control.

Internet se ha convertido en un elemento esencial para la vida de las personas. A las nuevas generaciones les cuesta imaginar un mundo sin conectividad y comunicación permanente. Una generación de "nativos digitales" ha crecido con conectividad ubicua, en donde ni fronteras ni idioma parecen ser barreras para la comunicación[1]. Poco a poco las constituciones de los países van reconociendo el acceso a las Tecnologías de la Información y Comunicación (TICs), de manera general, y a la Red, de manera particular, como un derecho fundamental y consagran en sus articulados el denominado "acceso universal", tal como en su momento lo hicieron con la educación y la salud[2].

Sin embargo, una gran mayoría de personas ignora todos los elementos necesarios que deben existir para que puedan comunicarse y conectarse a Internet.

1 John Palfrey and Urs Gasser (2008), *Born Digital: Understanding the First Generation of Digital Natives*, New York, Basic Books, 44-53.

2 La Constitución de la República del Ecuador (2008), dentro de los Derechos del Buen Vivir (Capitulo II), en su Sección III incluye en el Art. 16.2 "*El acceso universal a las tecnologías de la información y comunicación*" como un derecho que tienen todas las personas en forma individual o colectiva y en el Art. 17.2 dispone que el Estado facilite dicho acceso universal. Lo propio hace con la educación en el Art. 28 y con la salud en el Art. 32 y 362.

Se tienen nociones básicas de que la telefonía móvil tiene una infraestructura de antenas y células y que existen "proveedores de Internet" que prestan el servicio. Poco se conoce respecto a la infraestructura sobre la que se soporta la conectividad cotidiana o sobre los denominados recursos críticos de Internet[3] y mucho menos sobre el andamiaje jurídico y regulatorio sobre el que se asienta.

De manera muy sucinta, podemos decir que la conectividad y el acceso a Internet, independientemente de la plataforma que utilicemos, requiere de algunos elementos o componentes básicos: un dispositivo de conexión (equipos terminales-hardware), aplicativos para conectarse (software), una conexión (alámbrica o inalámbrica), un servicio de acceso a Internet (pagado o gratuito) y contenidos e información a los que accedemos (sitios Web, aplicaciones). Los elementos mencionados se complementan con otros menos conocidos para el común de los usuarios, estos permiten el funcionamiento mismo de Internet, procesan su tráfico e incluyen nodos, ruteadores, redes de fibra óptica, servidores raíz, servidores espejo, satélites, cables submarinos, antenas, recursos numéricos, protocolos, nombres de dominio, entre otros. Los primeros y los segundos tienen relación, en mayor o menor grado, con las telecomunicaciones por cuanto requieren o utilizan sus redes.

Igualmente, en la enunciación que hacemos de los elementos que permiten la conectividad y el acceso a Internet, también debemos mencionar una serie de actores que intervienen en la cadena de valor, tales como las operadoras de servicios de telecomunicaciones, de redes, de cable submarino, proveedores de capacidad satelital, carriers, proveedores del servicio de Internet, empresas integradoras, desarrolladores de aplicaciones, fabricantes de equipos, operadores virtuales, administradores de sistemas numéricos y nombres de dominio, usuarios, entre otros.

Identificados elementos y actores que cumplen determinados roles para posibilitar el acceso a Internet, concluimos que la denominada "industria" de las telecomunicaciones sobre la que funciona la Red es compleja y su análisis legal puede tener varias perspectivas que van desde modelos económicos, despliegue y compartición de infraestructura, hasta procesos regulatorios y contratos. La complejidad de esta industria ha sido una parte crítica de todas las controversias en política pública que surgen cuando los diferentes actores y participantes del sector tienen visiones y perspectivas distintas y adoptan posiciones que entran en conflicto y

3 El término "recursos críticos de Internet" es definido en el párrafo 13(a) del Reporte del Grupo de Trabajo en Gobernanza de Internet de Naciones Unidas (WGIG) como: "*la administración del sistema de nombres de dominio y direcciones de protocolo de Internet…, administración del sistema de servidores raíz, estándares técnicos, la comunicación entre pares (peering) y la interconexión, la infraestructura de telecomunicaciones, incluidas las tecnologías innovadoras y convergentes, así como también el multilingüismo*." A partir de ese momento, el término aparece en la Agenda de Túnez, párrafos 58, 70 y 72, adoptada en la Cumbre Mundial sobre Sociedad de la Información llevada a cabo en ese país en 2005.

que se derivan de la ambigua información disponible.[4]

Una de las primeras características económicas que distingue a las telecomunicaciones de la mayoría de industrias es que el valor del servicio de telefonía depende del número de gente (abonados) a los que puedo acceder a través de un servicio determinado (Brock, 1994). Un dispositivo de conexión, por más sofisticado que sea, si no tiene otros equipos similares con los que se pueda conectar, no tendría ningún valor. Esta característica se la conoce como externalidad de la red. A mayor cantidad de gente que puedo contactar a través de una red, mayor valor tiene la red[5]. De ese principio se deriva la importancia de la "interconexión" de las redes. Mientras más redes se interconecten, más personas pueden ser conectadas y contactadas, incrementando su valor e importancia. La interconexión se convierte así en uno de los elementos fundamentales de las telecomunicaciones y de su regulación, no solamente se vuelve un promotor de eficiencia, sino también un recurso que evita abusos y distorsiones de la competencia.

Existe una gran cantidad de operadores y redes, cada una de ellas cuenta con su infraestructura básica que debe ser susceptible de conectarse con otras redes de manera física (cables, switches, etc.) y de manera lógica (protocolos, lenguajes, números, etc.). Derivada de esta realidad, surge otra importante característica económica de las telecomunicaciones que consiste en los arreglos para compartir infraestructura y repartir ingresos derivados de los servicios. La transmisión de mensajes intangibles desde un emisor hasta un receptor, a través del telégrafo, teléfono, radio o satélite, depende de una serie de innovaciones tecnológicas fundamentales[6] que requieren de plataformas e infraestructuras que hagan posible su funcionamiento.

Aparte de las características económicas descritas, las telecomunicaciones también tienen características técnicas relacionadas con la calidad de servicio, tipos de red, anchos de banda y velocidad de transmisión, estas características son reguladas de manera general o a través de los contratos de prestación de servicios con el usuario final, en los que se establecen los índices de calidad, así como el ancho de banda disponible y los niveles de compartición del servicio de Internet contratado y soportado por servicios de telecomunicaciones.

Debemos recordar que a finales del siglo pasado, cuando Internet entró en un apogeo y entusiasmo desbordado por su proceso de masificación global, el acceso y la conectividad implicaban un precio de servicio que tenía dos componentes importantes: 1) la provisión del servicio mismo de Internet y 2) la del "servicio

4 Brock, G. (1994). *Telecommunication Policy for the Information Age: From Monopoly to Competition,* Cambridge/London: Harvard University Press, 11-18

5 Nuechterlein, Jonathan y Weiser, Philip J. (2005), *Digital Crossroads: American Telecommunications Policy in the Internet Age*, Cambridge/London, MIT Press, 7-15

6 Frischmann, Brett M. (2012), *Infrastructure: The Social Value of Shared Resources*, New York, Oxford University Press, Capítulo 10.

de última milla”[7]. La mayoría de abonados a Internet se conectaban vía telefónica (“dial-up”), a través de la línea de telefonía fija. La regulación de telecomunicaciones buscó esquemas que permitieron reducir las tarifas de acceso a Internet, para que el servicio pueda masificarse en la población. La “tarifa plana” fue una de las primeras estrategias regulatorias para abaratar el costo del servicio de telecomunicaciones requerido para acceder a Internet, lo que significaba que el abonado o usuario debía pagar un monto fijo por servicios de telecomunicaciones (llamada telefónica), sin considerar el tiempo que se conecte a Internet. Luego se desplegaron redes de cable coaxial que podían transmitir servicios de audio y video por suscripción y también ofrecer conectividad a Internet. Más adelante, surgió el denominado “Internet dedicado” que consistía en un servicio permanente de conexión con una línea dedicada para ese efecto. En la última década se desplegó una gran infraestructura de redes de fibra óptica y de tecnologías inalámbricas, tales como Wi-fi y Wi-max que, actualmente, se han consolidado, atribuyendo una gran importancia a la explotación y al uso del espectro radioeléctrico que ya venía siendo la base de la telefonía móvil.[8]

Esta evolución también se refleja en los cambios que sufre la definición de “telecomunicaciones”. Como dato curioso y didáctico, el Diccionario de la Real Academia de la Lengua Española[9] define todavía a las telecomunicaciones como un “*sistema de transmisión y recepción a distancia de señales de diversa naturaleza por medios electromagnéticos*”. Evidentemente, esta es una definición que ha sido ampliamente superada y afinada por la acelerada evolución tecnológica. Así, tenemos que hoy en día la definición de telecomunicaciones ha debido incorporar muchos más elementos, entre los que se destacan: intercambio de información por medios electrónicos y eléctricos, dispositivos de transmisión y recepción que evolucionan constantemente, procesos de modulación analógica o digital de ondas para trasmitir la información, entre otros elementos que abarca la definición actual de telecomunicaciones.

En el Ecuador las telecomunicaciones han tenido un proceso de transición de un modelo estatal, que tuvo el monopolio de la telefonía fija con varios modelos institucionales, a la liberalización del mercado de las telecomunicaciones a partir del año 2000. Efectivamente, el Instituto Ecuatoriano de Telecomunicaciones (IETEL), creado en 1972 y puesto a cargo del despliegue de la infraestructura física y prestación del servicio de telefonía fija, se convertiría en la Empresa Estatal de Telecomunicaciones (EMETEL), para más tarde ser objeto de un intento de modernización, previo a una pretendida privatización, escindiéndola en dos empresas regionales con carácter jurídico de “privadas” que fueron denominadas “Andinatel”

---

7 Ver: Lange, C., Behrens, C., Weis, E., Kraus, J., Krauss, S., Grigat, M., ... & Bogenfeld, E. (2016, April). Bridging the Last Mile. In Broadband Coverage in Germany; 10. ITG-Symposium (pp. 1-8)

8 Revisar Planes de Expansión de las operadoras de telefonía en Ecuador

9 http://www.rae.es/

y "Pacifitel"[10]. Los lectores recordarán que, en Ecuador, las primeras conexiones a Internet necesariamente requerían del servicio de las telefónicas estatales[11]. Finalmente, se las volvió a fusionar en una sola empresa denominada Corporación Nacional de Telecomunicaciones (CNT)[12], nombre que se mantiene hasta la fecha.

En el ámbito legal y regulatorio, la liberalización del sector de telecomunicaciones trae como consecuencias inmediatas, por un lado, el surgimiento de nuevos prestadores de servicios de telecomunicaciones, incluyendo telefonía fija[13], y, por otro, la necesidad de regulación que establezca normas para un mercado que se estaba reconfigurando. La interconexión de redes en Ecuador, al igual que en otros países, es uno de los principales retos para evitar distorsiones en el mercado, como las descritas al inicio del presente trabajo[14]. Igualmente, la entrada de un tercer operador de telefonía móvil, en 2003[15], se produjo bajo el régimen denominado "Servicio Móvil Avanzado ("SMA") que operaba en la banda de los 1900 MHz, mientras que los primeros dos operadores de telefonía móvil que obtuvieron la concesión por quince años, en 1993, lo hacían bajo el régimen denominado "Servicio de Telefonía Móvil Celular" ("STMC"), en la banda de 850 MHz. La principal ventaja tecnológica de la primera sobre la segunda radicaba en que la banda de 1900 MHz permitía la más eficiente transmisión de datos, además, los equipos de nueva generación funcionaban en esa banda[16]. Por su parte, la banda de 850 MHz

---

10 El Art. 48 de la Ley Especial de Telecomunicaciones, en reformas de 1995 y 1997, establece la modalidad en la que se produciría la "Delegación de la Explotación del Servicio de Telecomunicaciones al Sector Privado". Se contemplaba la escisión de EMETEL S.A. se pondría a la venta el 35% de las dos compañías resultantes de tal escisión. Sin embargo, ese proceso no llegó a concretarse.

11 Ecuanet, empresa del Banco del Pacífico, fue la pionera en ofrecer servicios de conexión a Internet en Ecuador, servicio que requería de una línea de telefonía fija y, por tanto, ya dependía del servicio estatal de telecomunicaciones.

12 El 30 de octubre del 2008, como resultado de la fusión de Andinatel S.A. y Pacifictel S.A., nace la CORPORACIÓN NACIONAL DE TELECOMUNICACIONES, CNT S.A. El 14 de enero del 2010, CNT S.A., se convierte en empresa pública, y pasa a ser la CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP

13 Ecuador Telecom (ECUTEL S.A.) y Servicios de Telecomunicaciones (SETEL S.A.) entran en 2002 al mercado ecuatoriano a prestar servicios de telefonía inalámbrica fija local, larga distancia nacional e internacional

14 El Reglamento de Interconexión fue expedido mediante Resolución CONATEL-602 en febrero de 2007 y publicado en el Registro Oficial 41 de 14 de marzo del mismo año y su última reforma fue en junio de 2012.

15 En diciembre de 2003 ingresa al mercado de la telefonía móvil el nuevo operador Telecsa S.A. que comercializa sus servicios bajo la marca "Alegro PCS" bajo el régimen del denominado "Servicio Móvil Avanzado" (SMA) operando en la banda de frecuencia de los 1900MHz.

16 En un inicio, la compañía concesionaria Telecsa S.A. entró al mercado con su marca "Alegro PCS (Personal Communication System). Sin embargo, en el año 2005 lanza al mercado ecuatoriano la tecnología CDMA 1X (EV-DO) en la banda de 1900 MHz, para ofrecer transmisión de datos y acceso móvil a Internet. Más adelante, en 2007, reemplazaría la tecnología CDMA, que le resultaba muy

era esencialmente para la transmisión de voz. Alegro PCS, de propiedad de las telefónicas estatales, estaba lista para introducir en Ecuador servicios de Internet móvil inalámbricos en una plataforma y banda muy eficientes para ese propósito[17].

Por esos mismos años se dictó la regulación para normar la prestación de servicios de Internet a través del denominado Reglamento para la Prestación de Servicios de Valor Agregado[18] (en adelante "RSVA"), a pesar de que la Ley Especial de Telecomunicaciones (en adelante "LET"), vigente en esa época, aún no hacía mención a ese tipo de servicios ni a Internet. El RSVA que definía a los servicios de valor agregado como "*aquellos que utilizan servicios finales de telecomunicaciones e incorporan aplicaciones que permiten transformar el contenido de la información transmitida*"[19] determina que sus prestadores requerirán de un permiso otorgado por un ente regulador de las telecomunicaciones como título habilitante. Resulta importante, para efectos de entender una de las conclusiones del presente artículo, recalcar que el Art. 1 del RSVA establece claramente que ese cuerpo normativo tiene por objeto establecer normas y procedimientos para la prestación del servicio de Internet "[…] *así como los deberes y derechos de los prestadores de servicios a sus usuarios* […]", sin que estos últimos estén sometidos a obligaciones que, algunos años más tarde, el Estado habría de imponer.

El RSVA también clarifica el rol de los denominados "servicios portadores" en la prestación de servicios de Internet, los mismos que el Art. 8 de la extinta LET los definía como aquellos que "*proporcionan la capacidad necesaria para la transmisión de señales entre puntos de terminación de red definidos*", es decir, aquellos que permitían físicamente que la información (datos) sea enviada y receptada. Para esos servicios se requería la obtención de un título habilitante bastante costoso.[20]

Si bien es cierto que el proceso de liberalización mencionado permitió el surgimiento de nuevos actores en el mercado de las telecomunicaciones, tanto operadores fijos como móviles y servicios portadores, así como una significativa inversión en una nueva tecnología para complementar los servicios de voz con el de datos (correo electrónico e Internet móvil), también es cierto que la posición de dominancia de algunos de ellos comenzó a generar ciertas distorsiones que no

---

costosa, por tecnología GSM, rentando redes del operador Otecel, que competía en el mercado de telefonía móvil con la marca "Movistar".

17 Las otras dos operadoras de telefonía móvil celular ya venían ofreciendo, de manera incipiente, servicios de datos, pero dadas las características de la banda en que operaban, todavía era muy lento el servicio y a precios que no hacían posible su masificación.

18 Resolución No. 071-03-CONATEL-2002 (RSVA)

19 Art. 2 RSVA (2002)

20 Los valores relacionados a la obtención del título habilitante de portador ascendían a casi medio millón de dólares, lo que lo convertía en otro elemento que contribuía a los altos costos del servicio de Internet en Ecuador.

pudieron ser fácilmente corregidas por la inexistencia de una ley de competencia en Ecuador. En el año 2006 hubo un intento de regulación de la competencia, específicamente para las telecomunicaciones, sin que se llegue a concretar, en gran medida por la resistencia que opusieron las operadoras dominantes. Ecuador debió esperar hasta 2011 para contar con la Ley Orgánica de Regulación y Control del Poder de Mercado. Hasta tanto, el mercado de las telecomunicaciones había seguido creciendo a ritmo exponencial, en cuanto a abonados y usuarios que siguen una tendencia global de expansión, acompañada de un avance tecnológico en cuanto a capacidad y velocidad de transmisión se refiere, así como también de dispositivos. La tendencia es marcada por los denominados “teléfonos inteligentes” que permiten y estimulan el crecimiento del servicio de Internet móvil.

Sin embargo, hacia 2006 las tarifas de acceso a Internet en Ecuador eran de las más elevadas de la región y tenían servicios de banda ancha que no alcanzaban ni el 1% de penetración en el mercado. Derivado de estudios[21] y del trabajo conjunto del sector privado[22] se llegó a la conclusión de que los dos principales factores que mantenían altos los costos de la provisión de Internet en Ecuador tenían relación directa con el sector de telecomunicaciones:

1) La saturación de tráfico de salida de Internet por el Cable Panamericano, el único con un punto de salida en Ecuador y la ausencia de nodos de conexión locales con otros cables submarinos que pasan frente a las costas ecuatorianas. Este factor no dejaba otra alternativa a los operadores de telecomunicaciones que sacar su creciente tráfico de Internet por Colombia y Perú, pagando altos costos de conexión y transporte del tráfico a través de carriers en esos países. Esos altos costos eran trasladados al usuario final.

2) La falta de regulación y coordinación, así como la duplicidad en la inversión y en el despliegue de infraestructura de redes, particularmente, de fibra óptica, hasta el punto de que existan tramos duplicados y hasta triplicados de tendido de fibra óptica, como entre Quito y Guayaquil, mientras que habían muchas poblaciones y zonas en donde esas redes de nueva generación ni siquiera habían llegado.

Frente a estos dos elementos, directamente relacionados con el ámbito de las telecomunicaciones, se requerían acciones de política pública y regulatorias que tengan un impacto positivo en los servicios de provisión de Internet en Ecuador. Es

21 El CONATEL encargó a la Asociación de Empresas de Telecomunicaciones de la Comunidad Andina (“ASETA”) un estudio-investigación en el mercado de provisión de servicios de Internet en Ecuador para determinar la composición de costos del servicio y establecer el valor de oportunidad de implementación de una nueva salida de cable submarino.

22 Los proveedores de servicios de Internet se aglutinan en la Asociación Ecuatoriana de Proveedores de Internet (“AEPROVI”) y los operadores de telecomunicaciones en la Asociación de Empresas de Telecomunicaciones (“ASETEL”). Ambas organizaciones participaron en mesas de análisis para determinar las principales razones que encarecían el precio final del servicio de Internet en Ecuador.

así como a finales de 2005, el órgano regulador de las telecomunicaciones (CONATEL) se puso en contacto con dos de los principales cables submarinos que pasan frente a costas ecuatorianas[23], para tratar de persuadirles de realizar inversiones y traer un punto de conexión desde sus cables hasta territorio continental ecuatoriano. Estos esfuerzos rindieron sus frutos cuando la empresa TEWS, a mediados de 2006, decidió realizar una inversión privada de aproximadamente cuarenta millones de dólares para traer, por lecho submarino, una extensión que conectaría al Ecuador con su cable submarino, permitiendo así que el tráfico de Internet de los usuarios ecuatorianos salga directamente y sin necesidad de hacerlo por los países vecinos.

Si bien es cierto que la prioridad de política pública en la administración saliente era lograr la inversión privada para conectar al Ecuador a una salida internacional adicional, y así brindar todas las facilidades e incentivos posibles al inversionista privado, una vez que se concretó e inició el proyecto de despliegue del cable hacia Ecuador, que coincidió con el cambio de gobierno en enero de 2007, la prioridad del gobierno entrante fue imponer ciertas obligaciones al operador del cable submarino. Efectivamente, el nuevo gobierno desestimó el borrador del proyecto de Reglamento para la Provisión de Capacidad de Cable Submarino que se venía trabajando en coordinación con el sector privado que participa en la cadena de valor para la provisión del servicio de Internet, y, en su reemplazo, se procedió a expedir en julio de 2007 un reglamento[24] en el que se imponían dichas obligaciones, esencialmente a la empresa de cable submarino entrante que había realizado la inversión, para entregar capacidad al Estado a título gratuito[25]. Si bien es cierto que resultó loable que el Estado haya exigido capacidad de cable submarino gratuita para educación y desarrollo social, el cambio súbito de las reglas y la imposición de nuevas obligaciones a un inversionista privado que había realizado un despliegue de infraestructura vital para el Ecuador, evidenciaba ya ese clima de incertidumbre e inseguridad jurídica que habría de ser una constante en el nuevo gobierno.

En este punto, cabe recordar que el Ecuador tenía prácticamente saturado el acceso al Cable Panamericano, al cual se accedía a través de la Estatal EMETEL, institución a la que nunca se le había exigido capacidad gratuita, ejemplo que corrobora ciertos tratos que la estatal de telecomunicaciones recibió a lo largo del tiempo, situación que también generaba una distorsión de la competencia en el mercado de las telecomunicaciones. Así, el Régimen de Tasas y Tarifas para Servicios de Telecomunicaciones aprobado en marzo de 1994, bajo el Capítulo de Servi-

23 Global Crossing y TEWS (empresa vinculada con Telefónica de España).

24 Resolución 347-17-CONATEL-2007, expedida el 14 de junio de 2007 y publicada en el Registro Oficial No.119 de 04 de julio de 2007

25 El Art. 16 de la Resolución 347-17-CONATEL-2007, en su segundo párrafo introduce la obligación del peticionario de entregar "*una determinada capacidad internacional con acceso a Internet para uso de desarrollo social y educativo en la estación terminal de cable submarino*".

cios de Arrendamiento, numeral 5.3.1.3, incluye el de "circuitos para la transmisión de datos", donde se establece que la infraestructura de la red pública de la estatal EMETEL podrá ser utilizada para "suministrar enlaces digitales" utilizando cables submarinos y/o fibra óptica, entre otras facilidades de su propiedad[26].

Paralelamente a lo que sucedía en Ecuador, según se relata en los puntos anteriores, entre 2005 y 2010 se produjeron dos fenómenos globales fundamentales que tienen una incidencia directa en el mercado de provisión de servicios de Internet en Ecuador: el vertiginoso crecimiento de la penetración de la telefonía móvil hasta alcanzar casi el 100% de penetración y la denominada "convergencia tecnológica" en la que proveedores de servicios de telefonía móvil y de televisión por suscripción utilizan su infraestructura física (redes de fibra óptica, coaxial, celular, satelital, etc.) y sus servicios para ofrecer acceso y conectividad a Internet. La virtud de la convergencia tecnológica consiste en permitir el acceso a Internet a través de varios tipos de servicios empaquetados comercialmente y de una multiplicidad de dispositivos que vienen con capacidad para conectarse a Internet.[27] Sin embargo, la legislación ecuatoriana se enfocaba en la regulación de servicios de telecomunicaciones, incluido Internet (valor agregado), en lugar de enfocarse en redes, sin considerar los dispositivos que utilice el usuario o abonado para recibir el servicio.

Aunque el gobierno de turno hablaba de un proceso de modernización de las telecomunicaciones, en su afán de universalizar el acceso a las TICs y masificar el uso de Internet, antes de aprobar una nueva ley para modernizar el sector, prefirió embarcarse en una reingeniería institucional que inició con la creación de un Ministerio de Telecomunicaciones y de la Sociedad de la Información[28] (en adelante "MINTEL"), cuyo decreto presidencial de creación también dispone la "fusión" del Consejo Nacional de Radiodifusión y Televisión (en adelante "CONARTEL") con el Consejo Nacional de Telecomunicaciones (CONATEL), con lo cual desaparecía al primero vía decreto, a pesar de que había sido creado por Ley.

Al MINTEL se le encarga la definición y formulación de políticas públicas relacionadas con Internet y a coadyuvar en la promoción de su uso, conjuntamente con otras atribuciones para impulsar el desarrollo de la Sociedad de la Información. El ministro de telecomunicaciones pasó a convertirse también en el Presidente del CONATEL, decisión que lamentablemente iba en sentido opuesto a la corriente global de contar con órganos de regulación y control independientes y técnicos. Al

---

26 EMETEL tenía prácticamente copada la capacidad de acceso al Cable Panamericano y no tenía ningún incentivo para facilitar el acceso a la infraestructura de salida de tráfico de Internet a sus competidores locales, con lo cual se generaba una distorsión al, todavía incipiente, mercado de provisión de Internet en Ecuador.

27 Los denominados "triple pack" consiste en el empaquetamiento de tres servicios con un mismo prestador, que usualmente ofrecía acceso a Internet combinado con telefonía móvil, telefonía fija, audio y video por suscripción, etc.

28 Decreto Ejecutivo 8 publicado en el Registro Oficial 10 de 24 de agosto de 2009.

ser presidido por un ministro de Estado, el CONATEL, que pasó también a regular radio y televisión, era subordinado directamente al Poder Ejecutivo, a través de un miembro de su gabinete ministerial y se corría el riesgo inminente de que políticas públicas propias del Ejecutivo se confundan con regulación y control que demandan total independencia. La consecuencia inmediata de este cambio institucional fue que el MINTEL no se limitó exclusivamente al ámbito de las políticas públicas, sino que tuvo total injerencia e influencia en la regulación y en el control de las telecomunicaciones, radio, televisión y la administración del espectro radioeléctrico.

El MINTEL puso especial énfasis en la instalación y en el equipamiento de los denominados "infocentros" como la base fundamental para el desarrollo de la Sociedad de la Información en Ecuador. En sintonía con la política del gobierno central de invertir en infraestructura de todo tipo (vial, eléctrica, aeroportuaria, etc.), el MINTEL y el FODETEL (Fondo de Desarrollo de las Telecomunicaciones), administrado por el primero, en colaboración estrecha con la estatal de telecomunicaciones CNT, desplegaron redes físicas de fibra óptica y dotaron de computadoras y conectividad a infocentros y escuelas. Lamentablemente, la infraestructura es solamente una parte del ecosistema que la Sociedad de la Información requiere para desarrollarse[29].

En lo referente a Internet, se evidencia un primer intento del gobierno por tratar de someter a sus usuarios y abonados a la regulación, originalmente destinada a los operadores y proveedores de ese servicio de valor agregado, cuando se dicta el Reglamento para los Abonados/Clientes-Usuarios de los Servicios de Telecomunicaciones y de Valor Agregado (en adelante "Reglamento Abonados")[30]. En los considerandos de la mencionada resolución se justifica la emisión de tales normas para garantizar el acceso universal a las TICs, consagrar el derecho de las personas a proteger sus datos personales, su privacidad y a obtener un servicio de calidad elegido libremente y con sujeción al contenido de los contratos de servicio suscritos. Sin embargo, los mismos considerandos ya introducen los elementos típicos y comunes de muchos gobiernos para abrir la ventana al control y monitoreo de los usos de Internet y de los flujos de información que transitan por la red, tales como la prohibición del uso de los medios de telecomunicación, incluido el Internet, "*contra de la seguridad del Estado, el orden público, la moral y las buenas*

29 Al igual que una carretera, autopista o aeropuerto que no adquiere valor si no existe previa o paralelamente la producción de bienes (agrícolas, industriales, etc.), turismo (infraestructura hotelera, turistas, feriados, etc.) y medios de trasporte (carros, camiones, aviones, etc.) que demanden esa infraestructura de vías, los infocentros desplegados, sin usuarios con conocimientos básicos en TICs, contenidos y aplicaciones locales, condiciones adecuadas de mercado, inversión tecnológica, legislación adecuada, entre otros, tampoco adquieren valor, serán inocuos y su equipamiento pronto será obsoleto para terminar convertido en chatarra tecnológica.

30 Resolución CONATEL-477 aprobado el 11 de julio de 2012 y publicada en el Suplemento del Registro Oficial 750 de 20 de julio del mismo año.

costumbres"[31]. Bajo tales consideraciones se reafirman derechos de los usuarios y abonados que ya estaban consagrados en la Constitución, la LET, la Ley Orgánica de Defensa del Consumidor, regulación sobre índices de calidad de los servicios de telecomunicaciones, entre otras normas, para los cuales no era necesaria una regulación especial. Sin embargo, invocando todos esos derechos preexistentes y para evitar supuestos abusos en contra de los usuarios (consumidores) en aspectos tarifarios y de promociones, se dictó el Reglamento de Usuarios.

Es así como el Art. 1 del Reglamento de Usuarios traza como propósito de la regulación la protección de los derechos de los usuarios, pero también la regulación de la relación de estos con los proveedores de los servicios de Internet. Se confirman e instrumentan entonces una serie de derechos de los usuarios y se esbozan, de manera bastante incipiente aún, los principios de neutralidad de la red[32] y neutralidad tecnológica[33]. Lo interesante de esta regulación es que, en mi opinión, esos principios incipientes de neutralidad nacen con excepciones bastante ambiguas, peligrosa situación que tres años más tarde sería confirmada y consagrada en la nueva ley de telecomunicaciones. Es mi personal percepción, derivada del análisis jurídico de la norma, mencionar que ya existía ese momento la intención del gobierno de regular las relaciones entre proveedores y abonados de servicios de Internet, en un afán de identificar usuarios y monitorear flujos de información[34], pero sin encontrar todavía la fórmula precisa.[35]

La asignación de un poder tan amplio, que incluye la suspensión de principios básicos y derechos constitucionales como el de la privacidad y protección de datos personales, a una "autoridad competente" que no es definida ni especificada en ninguna parte, resulta una ambigüedad jurídica que acarrea riesgos enormes para

---

31 El Reglamento de Abonados, en sus considerandos invoca el Art. 11 de la Ley Especial de Telecomunicaciones Reformada.

32 La neutralidad de la red la representa el numeral 15.6 del Art. 15 del Reglamento de Abonados que consagra como derecho de los abonados/clientes-usuarios a "*hacer uso de cualquier aplicación o servicio legal disponible en la red de Internet, con lo cual el ser vicio que ofrezcan los prestadores de los servicios no deberán distinguir ni priorizar de modo arbitrario contenido, servicios, aplicaciones u otros, basándose en criterios de propiedad, marca, fuente de origen o preferencia.*"

33 La neutralidad tecnológica está más orientada a aparatos, equipos y dispositivos de acceso. El Reglamento de Abonados la incluye como derechos "de libertad", cuando en el numeral 14.4 del Art. 14 lo define como "*escoger libremente el equipo terminal en el que recibirá los servicios contratados, siempre y cuando los equipos elegidos cumplan con las normas de homologación establecidas para el efecto*". Esto es complementado con la obligación del prestador de los servicios que, conforme lo dispone el numeral 34.1 del Art. #4 del Reglamento de Abonados, debe "*abstenerse de exigir el uso exclusivo de determinado equipo para la prestación de servicios contratados por el abonado/cliente…*"

34 Ver Arts. 37, 38 y 39 del Reglamento de Abonados.

35 El Art. 41 prohíbe a los prestadores de servicios de Internet "*bloquear, priorizar, restringir o discriminar de modo arbitrario y unilateral aplicaciones, contenidos o servicios sin consentimiento del abonado/usuario-cliente o por orden expresa de la autoridad competente*".

los derechos y garantías de los usuarios de Internet. En el Reglamento de Abonados, esa autoridad indefinida puede solicitar datos personales de los usuarios, sin necesidad de su consentimiento o conocimiento previo.[36] Más adelante analizaré las graves connotaciones legales que tiene esta situación ratificada en la nueva ley de telecomunicaciones. Sin embargo, en el Reglamento de Abonados se introducen y consagran dos elementos más del control sobre usuarios de Internet que son: el empadronamiento de usuarios y las bases de datos de equipos terminales para determinar con exactitud la identidad de los usuarios de la red, completándose el propósito de identificación personalizada del usuario. Cabe mencionar en este punto que entre las atribuciones asignadas al ministro de telecomunicaciones en el decreto ejecutivo de creación del MINTEL, también se incluye plenas potestades para la creación y regulación de la "Central de Datos del Ecuador" que incorpora el intercambio de información por medios electrónicos y que más adelante derivaría en el Sistema Nacional de Registro de Datos Públicos (SINARDAP), cuya dirección está adscrita a ese ministerio.

En línea con lo anterior, no se puede dejar de mencionar, aunque sea de manera sucinta, la siguiente iniciativa de regulación de Internet cuando el Ejecutivo busca complementar las normas de telecomunicaciones con artículos de la Ley Orgánica de Comunicación, cuyo controversial e intrincado proceso de aprobación en Ecuador por parte de la Asamblea Nacional tomó cerca de cuatro años y en donde se pretendió ampliar el ámbito de aplicación de dicho cuerpo normativo a "*cualquier plataforma tecnológica*" para efectos de controlar y regular contenidos en Internet.[37]

Atravesando aguas turbulentas expresadas en ataques, críticas y amenazas de estricta regulación emanadas por el mismísimo Presidente de la República, Internet en Ecuador navega sin normativa clara y sin que su legislación se modernice adecuadamente, consagrando seriamente los principios de neutralidad tecnológica y de la red. Esta situación entiendo se derivó de una creciente incomodidad, sin que sea un efecto local, sino global, que generó en autoridades y dignatarios del

---

36 Ver Arts. 20, 30.5, 35.1 y 41

37 En el Proyecto de Ley Orgánica de Comunicación publicado en medios de comunicación el 07 de febrero de 2012, el Art. Art. 4 considera como medio de comunicación social sometido a esa ley a "*empresas y organizaciones públicas y privadas o comunitarias que presten el servicio público de comunicación masiva usando como herramienta cualquier plataforma tecnológica*". Más adelante, en el borrador presentado por la Comisión de Comunicación al Presidente de la Asamblea Nacional el 04 de abril de 2012, se lo modifica para aclarar en el Art. 4 que "*esta ley no regula la información u opinión que circula a través de las redes sociales*", con lo que se dejaría exenta de la regulación a esos servicios. Sin embargo, en el Art.5 del proyecto que define medios de comunicación social, se menciona que son todos aquellos que "*prestan el servicio público de comunicación masiva usando como herramienta medios impresos o servicios de radio, televisión y audio y video por suscripción, cuyos contenidos puedan ser generados o replicados por el medio de comunicación o a través de Internet*". Finalmente, luego de una firme oposición, el texto de la Ley Orgánica de Comunicación fue aprobado y promulgado y eliminó las referencias a "plataformas tecnológicas" e Internet.

poder público el empoderamiento social y la participación ciudadana a través de Internet, sus plataformas, aplicaciones y servicios. Las redes sociales facilitaron la circulación de información, la movilización social, el ejercicio de la libertad de expresión y el escrutinio público permanente a políticos, funcionarios y personajes públicos. En ese contexto, llegamos a la actualidad con un nuevo escenario de las telecomunicaciones en el ámbito normativo e institucional que incide directamente en Internet.

Una vez que la convergencia tecnológica se impone como un fenómeno global e incontrolable, marcado por la evolución de equipos y dispositivos cada vez más poderosos, funcionales y asequibles a la mayoría de usuarios en el mundo, una vez que la movilidad se convierte en una demanda de los usuarios, se reafirma la ubicuidad de Internet, se masifica el uso de la nube (“cloud”) y se van haciendo cada día más complejos los aspectos de jurisdicción y ley aplicable, entonces la legislación local de cada país no tiene otra opción que modernizarse y ser sensible a las nuevas realidades de Internet y de sus usuarios. Sin embargo, conforme crece el significado y la influencia política de Internet, los estados tienden a desarrollar una “arquitectura de control” a través de tecnología, regulación, normas y cálculos políticos, con el objeto de modelar un nuevo panorama geopolítico de la información[38].

Efectivamente, durante la década pasada, muchos estados desarrollaron estrategias legales, regulatorias y técnicas para negar el acceso mediante Internet a ciertos contenidos indeseables. Surgen los primeros sistemas para filtrar contenidos y China se convierte en uno de los ejemplos más representativos[39]. En el caso de China, el mecanismo para filtrar consistía en listas de direcciones IP, palabras clave y/o nombres de dominio programados en ruteadores o en paquetes de software que se situaban en puntos estratégicos de tráfico de Internet, típicamente los puntos de salida internacional o en los proveedores de Internet más grandes[40]. Estas iniciativas y estrategias constituyeron la primera generación de las técnicas para controlar Internet que poco a poco se fueron expandiendo, justificadas en la lucha contra el terrorismo, la pornografía infantil y la ciberseguridad, hasta ser algo de lo que se discute abiertamente en nuestros días.

Esta primera generación de técnicas para controlar Internet ha buscado convertirse en parte normal y aceptable de la legislación y regulación de los países a través de varios mecanismos para ejercer el poder estatal en el ciberespacio. En el caso de Ecuador, la legislación de telecomunicaciones constituye piedra angular de

38 Deibert, Ronald; Palfrey, John; Rohozinski, Rafal; Zittrain, Jonathan (editores) (2010), *Access Controlled: the shaping of power, rights and rule in Cyberspace*, Cambridge/London, The MIT Press

39 En el caso de China se denominó “Great Firewall of China” convirtiéndose en uno de los casos más paradigmáticos de censura en Internet.

40 Steven J. Murdoch and Ross Anderson, “Tools and Technology of Internet Filtering”, in *Access Denied: The Practice and Policy of Global Internet Filtering, ed. Ronald J. Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain (2008), Cambridge/London, The MIT Press, 57-72.*

esos propósitos, la misma que, combinada con otras estrategias de aplicación de leyes convencionales y presión política, permite ejercer una gran influencia sobre proveedores, usuarios y contenidos de la Red.

La nueva Ley Orgánica de Telecomunicaciones[41] (en adelante "LOT") aprobada en Ecuador, en febrero de 2015, introduce algunos cambios sustanciales como orientarse al modelo de regulación de las redes en lugar de los servicios. Hoy en día, con una red de fibra óptica o inalámbrica pueden prestarse muchos servicios, aparte de Internet. Sin embargo, los aspectos positivos de la LOT se ven empañados por una antitécnica reforma institucional que lleva a una inminente politización del manejo de las telecomunicaciones y por una inadecuada incorporación de los principios de neutralidad de la red y neutralidad tecnológica que, siguiendo el mismo patrón del Reglamento Usuarios analizado anteriormente, ratifica ambiguas y peligrosas excepciones a esos principios y derechos fundamentales de los usuarios de Internet. Igualmente, se profundiza el afán de controlar a los usuarios y someter a los proveedores del servicio de Internet a decisiones de autoridad competente que pueden comprometer severamente la privacidad y los datos personales de los usuarios, así como restringir la libertad de expresión y de información.

Efectivamente, el Art. 23 de la LOT consagra los derechos de los abonados, clientes y usuarios de los servicios de telecomunicaciones y en el numeral 18 desarrolla el principio de neutralidad de la red al establecer:

> A acceder a cualquier aplicación o servicio permitido disponible en la red de internet. Los prestadores no podrán limitar, bloquear, interferir, discriminar, entorpecer ni restringir el derecho de sus usuarios o abonados a utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación, desarrollo o servicio legal a través de internet o en general de sus redes u otras tecnologías de la información y las comunicaciones, ni podrán limitar el derecho de un usuario o abonado a incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos en la red, siempre que sean legales. Se exceptúan aquellos casos en los que el cliente, abonado o usuario solicite de manera previa su decisión expresa de limitación o bloqueo de contenidos, aplicaciones, desarrollos o servicios disponibles, o por disposición de autoridad competente. Los prestadores pueden implementar las acciones técnicas que consideren necesarias para la adecuada administración de la red en el exclusivo ámbito de las actividades que le fueron habilitadas, para efectos de garantizar el servicio.

Como se evidencia, el mismo numeral establece la excepción al principio, dejando que sea la "autoridad competente", que bien podría ser un ministro o cualquier otro funcionario de rango administrativo, quien ordene al proveedor del servicio

---

41 La Ley Orgánica de Telecomunicaciones fue publicada en el Tercer Suplemento del Registro Oficial 439 el 18 de febrero de 2015.

bloquear, restringir, limitar o suspender el servicio o el acceso a determinados contenidos y/o aplicaciones que esa autoridad los considere atentatorios a la seguridad interna o contrarios a cualquier otra norma, incluso de regulación. Se sugirió durante el debate de la LOT que se reemplace "autoridad competente" por "juez competente", pero se hizo caso omiso a tal sugerencia. La justicia, respetando las garantías del debido proceso, siempre ha tenido la potestad de suspender y/o restringir derechos, la autoridad administrativa no. Adicionalmente, todo lo descrito se enmarca en un escenario de ausencia de una Ley de Privacidad y Protección de Datos Personales en el Ecuador[42] y en un contexto marcado por casos emblemáticos como el de Edward Snowden que reveló la forma como el Estado vigilaba y espiaba a ciudadanos masivamente.

Lo descrito en el párrafo anterior tiene concordancia con los artículos 24 y 25 de la misma LOT, donde se abordan las obligaciones y los derechos de los prestadores de servicios de telecomunicaciones y se ratifica la excepción otorgando a la "autoridad competente" la capacidad para ordenar la limitación y hasta la anulación del principio de neutralidad de la red y la libertad tecnológica para utilizar cualquier dispositivo o equipo que no esté prohibido por la ley. Para completar la delicada situación de desprotección del usuario, el Art. 85, que establece las obligaciones adicionales de los prestadores de servicios, le otorga a la poderosa Agencia de Regulación y Control de las Telecomunicaciones (en adelante "ARCOTEL"), adscrita al MINTEL y controlada por el Ejecutivo, la competencia para establecer y reglamentar los mecanismos para supervisar el cumplimiento de las obligaciones referidas al secreto de la comunicaciones, así como la seguridad de datos personales, teniendo incluso la potestad de dictar "[…]*las instrucciones correspondientes, que serán vinculantes para las y los prestadores de servicios* […]", entre las que constan la obligación de proporcionar información acerca de la políticas de seguridad e integridad que puede incluir una auditoria a sus sistemas por parte de la autoridad administrativa.

Bajo el mismo formato que adopta el Reglamento Abonados, la LOT evidencia una clara intencionalidad de imponer controles a los usuarios bajo el formato de obligaciones que deben ser asumidas como contraprestación a los derechos que supuestamente consagra y le otorga la Ley al usuario de los servicios de Internet. Sin embargo, reitero que todos los derechos que supuestamente otorga la LOT ya existían en otras normas jurídicas preexistentes. Sin que se priorice una muy necesaria legislación de protección de la privacidad y de datos personales, el Art. 23 de la LOT ordena al usuario a *"[c]umplir con las obligaciones de empadronamiento o registro de identidad, tales como proporcionar sus datos personales de identificación asociados a la línea o número telefónico, de conformidad con las regulaciones que*

42 La Asamblea Nacional del Ecuador se encuentra actualmente discutiendo un proyecto de Ley de Protección de Datos y Privacidad, cuyo borrador, en mi opinión personal, tiene graves deficiencias y está orientado más bien a cerrar el anillo de control del Estado sobre el ciudadano. El proyecto aún no ha pasado a primer debate del Pleno.

se dicten al respecto." (LOT, 2015). Nuevamente, el enfoque consiste en lograr una identificación total y precisa del abonado y del dispositivo que utiliza para hacer llamadas y conectarse a Internet.

A pesar del riego descrito en el párrafo anterior, la LOT establece en su Art. 2 que el ámbito de aplicación de la ley abarca "*todas las actividades de establecimiento, instalación y explotación de redes, uso y explotación del espectro radioeléctrico, servicios de telecomunicaciones y a todas aquellas personas naturales o jurídicas que realicen tales actividades a fin de garantizar el cumplimiento de los derechos y deberes de los prestadores de servicios y usuarios.*". Adicionalmente, el mismo artículo somete también a la ley a las redes e infraestructura usadas para la prestación de servicios de radiodifusión sonora y televisiva y a las redes e infraestructura de los sistemas de audio y vídeo por suscripción. Queda claro que los usuarios de los servicios de telecomunicaciones e Internet no se hallan sometidos a la LOT.

Sin embargo, el Presidente de la República, mediante Decreto Ejecutivo 864 de 28 de diciembre de 2015, dictó el Reglamento General a la LOT[1] y en su Art. 2, referido también al ámbito de aplicación, estableció que, tanto la LOT, como el mencionado reglamento, son de aplicación obligatoria en todo el territorio nacional para las personas naturales y jurídicas que realizan actividades de operación y provisión de servicios de telecomunicaciones, pero en el segundo numeral del artículo establece que ambos cuerpos normativos son también aplicables a:

a) Los usuarios del régimen general de telecomunicaciones.

b) Las personas naturales y jurídicas no poseedoras de títulos habilitantes que pudieren incurrir en las infracciones tipificadas en la Ley.

Toda vez que un reglamento no puede modificar ni ampliar el ámbito de aplicación de una ley, esta inclusión de los usuarios de los servicios de telecomunicaciones, incluido Internet, y de toda persona que pudiese incurrir en una infracción tipificada en la Ley, vía reglamento, resulta a todas luces arbitraria e improcedente.

Respecto a la reforma institucional que introduce la LOT, al crearse la ARCOTEL se eliminan CONATEL, Secretaria Nacional de Telecomunicaciones (SENATEL), que eran los órganos técnicos de regulación de las telecomunicaciones y los servicios de Internet y, más grave aún, se elimina a la Superintendencia de Telecomunicaciones (SUPERTEL), órgano técnico de control que pertenecía al Poder de Participación Ciudadana y Control Social. Cualquier racionalización o reingeniería institucional debía contemplar una entidad a cargo de las políticas públicas que proyecte los planes y la visión ideológica de un gobierno determinado, tal como el MINTEL y un órgano de regulación y control de carácter técnico y con total independencia del Poder Ejecutivo que pueda adoptar las medidas adecuadas para alcanzar un mercado de telecomunicaciones sano y con suficientes incentivos para promover

1 Suplemento del Registro Oficial No. 676 de 25 de enero de 2016.

la inversión en tecnología, redes y demás infraestructura; que se administre, asigne y concesione el espectro radioeléctrico de manera transparente y técnica para estimular la expansión de la conectividad en formatos inalámbricos y el uso de bandas libres sin mayores trabas para permitir la expansión del Internet de las Cosas (IOT); que se evite lo que se denomina "captura reguladora", situación en la que puede caer el órgano regulador por presión y/o influencia de intereses creados, de manera general, o la intervención de actores monopólicos muy poderosos que deberían ser controlados por el regulador[1] de un mercado que se caracteriza por una acelerada innovación tecnológica y una competencia desenfrenada, de manera particular.

Debemos reconocer que los aspectos de acceso a las TICs, la masificación de Internet, el acceso a recursos críticos y el fomento al desarrollo de contenidos locales han tenido un gran avance, esencialmente por la labor de la industria y del sector privado que ha desarrollado tecnología de punta y con precios accesibles para su masificación. Cada día es más común ver un teléfono inteligente o una tableta en manos de jóvenes y adultos de todos los estratos sociales. Emprendedores y visionarios han desarrollado aplicaciones y contenidos enfocados en mercados y necesidades locales. Los modelos colaborativos de desarrollo, trabajo y hasta de financiamiento se van consolidando. Las sociedades ya no esperan infocentros ni subsidios para la compra de dispositivos, sino una normativa que garantice la privacidad, que proteja la información personal, que consolide la libertad de expresión, que combata la cibercriminalidad, que estimule las transacciones electrónicas y que, en el sector de las telecomunicaciones, cree las condiciones adecuadas en el mercado para estimular la innovación y actualización tecnológica de prestadores de servicios, que incentive la inversión y el despliegue de redes y que corrija distorsiones y abusos de posición de dominancia, para evitar el surgimiento de nuevos monopolios a los que un sector tan dinámico ha demostrado ser propenso.

Muchas de las amenazas y riesgos que se ciernen sobre Internet tienen su punto crítico en el sector de telecomunicaciones. Elementos como un equilibrado ejercicio de la anonimidad y la lucha contra los ciberdelitos, respetando la privacidad de los usuarios, son retos de normativa eminentemente técnica. El desarrollo de perfiles de usuarios, tendencias de consumo, condiciones abusivas de uso de aplicaciones y servicios, la corrección de distorsiones de mercado con plataformas de mensajería instantánea excluyentes y que no se interconectan con competidores más pequeños, entre otros, son retos que tienen por delante las autoridades de telecomunicaciones en el Ecuador y en otras jurisdicciones. Sin embargo, si la tensión que causa en el poder político la inusitada influencia que adquiere Internet, redes sociales y usuarios trae como consecuencia la injerencia e imposición de esos intereses creados sobre la regulación técnica e imparcial que demanda Internet, entonces el panorama luce oscuro e incierto.

1 Del Bo, Ernesto (2006), Regulatory Capture: A Review, 22(2), Oxford Rev. of Economic Policy, 203-25.

Régimen de Contratación Privada en Internet* -Una aproximación local-

Vladimir Villalba Paredes
Universidad San Francisco de Quito

RESUMEN: Nuevas tecnologías en la contratación ha demandado un régimen particular para una nueva complejidad. El trabajo levanta la matriz actual de la normatividad prescriptiva de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos, en paralelo con la ley sustantiva civil y mercantil contractual, subordinada a la Ley Orgánica de Defensa del Consumidor. El fenómeno de la autenticidad del sujeto y contenido de la oferta y aceptación, la desmaterialización de mensaje de datos, la patología contractual y remedios previstos, bajo una visión crítica, es identificado en todo momento.

PALABRAS CLAVE: Comercio electrónico / Oferta y aceptación electrónica / Protección al Consumidor / Desmaterialización de mensajes.

ABSTRACT: New contractual technologies has demanded a special regime for a new complexity. This paper raises the current scheme of the Statute of Electronic Commerce, Electronic Signatures and Data Messages, in parallel with the contractual civil and comercial law, subordinate to the Organic Law on Consumer Protection. The phenomenon of the authenticity of the author and content of the offer

*Macarena Bahamonde contribuyó como Jefe de Investigación.

and acceptance, dematerialisation of message data, contractual pathology and remedies under a critical view is identified at all times.

KEYWORDS: Electronic Commerce / Electronic Offer and Acceptance / Consumer Protection / Dematerialisation of Message data.

Terminología:

COMELEC:	Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos
CCivil:	Código Civil de la República del Ecuador.
CComercio:	Código de Comercio de la República del Ecuador,
DECONSU:	Ley Orgánica de Defensa del Consumidor

I. Formación del Consentimiento

Cualquier vínculo jurídico inter-partes requiere esencialmente[2] el acuerdo mutuo, libre e informado, independientemente a la modalidad, formalidad o técnica empleada para alcanzar el acuerdo. A su vez, el acuerdo es la concreción bilateral de la voluntad individual de cada parte sobre los elementos esenciales del tipo contractual (tipología) o, a falta de prescripción normativa, sobre los elementos necesarios mínimos para identificar las prestaciones debidas.

Con carácter previo, la información ha de referirse a: las características principales de los bienes o servicios, el precio y los costos adicionales, las modalidades de pago, los derechos y obligaciones del consumidor, así como los procedimientos para anular un contrato y exigir indemnización. (Rivero, 2002, p.119)

El paradigma de perfeccionamiento del contrato no se modifica por el hecho de emplear la plataforma internet; por el contrario, la herramienta genera información (presunción) sobre autenticidad, contenido de la oferta y su aceptación, medio de pago y más, que depende a su vez de contratación a través de *webpage* (*eCommerce*) o simple correspondencia electrónica (*email*).

Y aún dentro de este tipo de contratos [contrato electrónico] podría distinguirse entre los que se celebran por medio del correo electrónico, donde las partes manifiestan a través del uso del lenguaje convencional y de la escritura su consentimiento, y aquellos en que la aceptación se manifiesta pulsando en un lugar señalado «ad hoc», *cliqueando* en un botón o icono en el que se incluyen las expresiones «OK» o «aceptar» (o la expresión de la tecla «enter»), por ejemplo en una página web que funciona como tienda virtual [...] (Pardo, 2003, p.50)

1 Independientemente al *battle of forms*, el consentimiento se manifiesta por acto verbal, solemne o real, según los casos.

1. Perfil de la oferta

La oferta en plataforma internet es la manifestación visual (o, eventualmente, audible) del originador de la construcción de la contratación, a lo cual agrega su voluntad de vincularse frente a la aceptación correspondiente a los términos, condiciones y limitaciones constantes sea en la *webpage* o sea en el email inicial o cadena.

La oferta debe contener la materia esencial y, eventualmente, accidental sobre la cual recaerá la aceptación. Así, en tratándose de una compraventa (mobiliaria), la primera radicará en la determinación de la cosa y el precio y, la segunda, en modalidades obligacionales como una condición, plazo o modo, así como particularidades de entrega o de pago[3].

La COMELEC no se refiere (ni tenía porqué referirse) al régimen del contenido de la oferta. Por el contrario, se deja a la libertad contractual el desarrollo del mercado (*Cfr.* Constitución Art. 66, 16). Por lo mismo, la policitación a través de plataforma internet se sujeta a los principios generales[4] y particulares[5] de la contratación[6].

En el caso de contratación mediante oferta a persona indeterminada (al público), principalmente a través de una *webpage*, el régimen paralelo que se dispara es el establecido en la DECONSU.

Esto se explica porque, como la cuestión "afecta a una gran parte del ordenamiento", una ley única sería "inviable desde el punto de vista técnico jurídico"; y en él "la intervención legislativa y la administrativa se encuentran en una condición de recíproca complementariedad. (Brizzio, 2001, p. 55)

Así, la matriz normativa (como una limitación a la autonomía de la voluntad) se presenta de la siguiente manera:

1.1 Entendido que la oferta busca una aceptación a un contrato de adhesión,

[…] deberá estar redactado con caracteres legibles, no menores a un tamaño de

---

2 A esto hay que agregar los elementos de la naturaleza en el caso de contrato típico o reglado.

4 Básicamente el principio de la autonomía de la libertad neutralizado por derechos de protección al consumidor.

5 Por regla general, la oferta no es vinculante, salvo el caso de oferta en firme (CComercio, Art.143) y la oferta a persona indeterminada (CComercio, Art. 148). Dentro del régimen de la oferta en el código de comercio, no se reconoce expresamente la doctrina del *promissory stoppel*.

6 Y al desarrollo *in-extenso* por la doctrina comparada y jurisprudencia local.

fuente de diez puntos[7], de acuerdo a las normas informáticas internacionales[8], en términos claros[9] y comprensibles[10] y no podrá contener remisiones a textos o documentos que, no siendo de conocimiento público, no se faciliten al consumidor[11] previamente a la celebración del contrato. [DECONSU, Art. 41 (1)]

1.2 Entendido que la oferta se manifiesta de manera escrita,

> […] deberán estar escritos en idioma castellano, salvo aquellas palabras de otro idioma que el uso[12] haya incorporado al léxico. [DECONSU, Art. 42 (1)][13]

1.3 Así mismo, el régimen preceptúa el efecto de "nulidad de pleno derecho[14] y no producirán efecto alguno[15]" las cláusulas que

1° Eximan, atenúen o limiten la responsabilidad de los proveedores por vicios[16] de cualquier naturaleza de los bienes o servicios prestados; [DECONSU, Art. 43 (1°)]

---

7 La norma preceptúa el efecto "no escrito" a los textos escritos "significativamente más pequeños". Parecería entenderse, por lo mismo, textos con fuente menor a 10 puntos, aunque la adjetivación puede dar pie a lectura diferente, aunque más sofisticada.

8 Resulta extraño el término "normas informáticas internacionales". ¿Acaso se refiere al reconocimiento internacional de los caracteres del abecedario latino?

9 La claridad está dada por el significado natural de la palabra, el uso comercial o el técnico atribuido por el arte (en el orden), dentro del contexto.

10 Lo comprensible debe entenderse como la información que razonablemente cualquier receptor obtiene de la oferta.

11 En contratación electrónica los textos adicionales pueden estar en *attachments* (en modalidad *email*) o en *hiperlinks* (en modalidad *eCommerce*), los cuales deben reunir los caracteres de ser claros y comprensibles también.

12 La prueba de la incorporación al léxico de un término extranjero por el uso es un hecho. En este sentido, ¿debe probarse?

13 La norma preceptúa el efecto "no escrito" de las cláusulas que no cumplan con este requisito (aunque la norma hace mención a "requisitos"). El efecto pudiera tener un alcance mayor a la simple cláusula, principalmente cuando sobre la palabra extranjera (que no siendo parte del léxico) gira el cumplimiento de la prestación; o un efecto menor, cuando la palabra puede ser sustituible por la naturaleza del contrato o fácilmente traducible.

14 Aunque la nulidad de pleno derecho es un avance jurisprudencial del Tribunal de Casación para los casos de manifiesta ilicitud del objeto o la causa, la norma incorpora la noción para el caso.

15 Nótese que hay redundancia entre el efecto de la "nulidad de pleno derecho" y "que no produzca efecto alguno". La nulidad de pleno derecho implicaría que la cláusula no llego a tener valor jurídico alguno. Lo anterior, sin perjuicio de reconocer que la misma expresión "nulidad de pleno derecho" resulta contradictoria: la nulidad presupone existencia de un efecto.

16 Modifica la regla general del carácter de elemento de la naturaleza (renunciable) del saneamiento por evicción (Art. 1782 CCivil) vicio redhibitorio (Art. 1799 CCivil) en la compraventa civil y de la compraventa mercantil (Art. 191 CComercio).

2° Impliquen renuncia a los derechos[17] que esta Ley reconoce a los consumidores o de alguna manera limiten su ejercicio; [DECONSU, Art 43, 2°]

3° Inviertan la carga de la prueba en perjuicio del consumidor[18]; [DECONSU, Art. 43 (3°)]

4° Impongan[19] la utilización obligatoria de un arbitraje o mediación, salvo que el consumidor manifieste de manera expresa[20] su consentimiento; [DECONSU, Art. 43 (4°)]

5° Permitan al proveedor la variación unilateral[21] del precio o de cualquier condición del contrato; [DECONSU, Art. 43 (5°)]

6° Autoricen exclusivamente al proveedor a resolver unilateralmente el contrato22, suspender su ejecución o revocar23 cualquier derecho del consumidor nacido del contrato, excepto cuando tal resolución o modificación esté condicionada al incumplimiento imputable al consumidor24; [DECONSU, Art. 43 (6°)]

7° Incluya espacios en blanco25, que no hayan sido llenados o utilizados antes de que se suscriba el contrato, o sean ilegibles; [DECONSU, Art. 43 (7°)]

8° Impliquen renuncia por parte del consumidor de los derechos procesales consagrados en esta Ley, sin perjuicio de los casos especiales previstos en el Código de Procedimiento Civil[26], Código de Comercio, Ley de Arbitraje y

---

17 Básicamente son derechos sobre los términos de contratación, políticas de crédito y cobranza, y devolución.

18 Lo cual internaliza el costo en el precio frente a la externalidad del costo de transacción.

19 El alcance de la patología es difusa, sobretodo tratándose de un contrato de adhesión vía plataforma internet.

20 Por su naturaleza, el de arbitraje es expreso, cuya voluntad se manifiesta en el *click* del *check out*.

21 La aplicación debe entenderse sobre una cosa determinada o determinable. Tratándose de servicios (tracto sucesivo), el ajuste eventual responde al principio de equilibrio económico del contrato. Una interpretación contraria llevaría a limitar la prestación con un plazo.

22 Implícitamente se está restringiendo el pacto de arras promisorias, penitenciales o de retractación, inclusive existiendo causa razonable.

23 La revocación es la terminación de un negocio jurídico unilateral. El término no se ajusta a un contrato (salvo el caso del mandato). Quizá la expresión "desconozca" se ajusta mejor.

24 No es más que el derecho a la resolución frente al incumplimiento contenido en la condición resolutoria tácita (Art. 1505 CCivil; Art. 198 CComercio).

25 Presupone una contratación mediante un formato escrito pre-impreso. En la modalidad *eCommerce* o mediante email no es aplicable, más todavía cuando previa a la aceptación la información de la contratación está "costumizada".

26 Hoy Código General de Procesos.

Mediación y demás leyes conexas[27]; y,

9° Cualquier otra cláusula o estipulación que cause indefensión al consumidor o sean contrarias al orden público y a las buenas costumbres[28]; [DECONSU, Art. 43 (9°)].

1.4 En tratándose de promoción u oferta especial, la DECONSU, Art.46 (1) preceptúa que la oferta debe contener el precio anterior y el nuevo precio del bien o servicio, o el beneficio que obtendría el consumidor.

1.5 En tratándose de sorteos o premios por consumo, la DECONSU, Art. 46 (2) preceptúa la obligatoriedad de determinar el número de premios, el plazo y lugar de retiro, así como la difusión adecuada del resultado.

1.6 La información del sistema de crédito está referida en detalle en la DECONSU, Art. 47 [Sistemas de Crédito]:

Cuando el consumidor adquiera determinados bienes o servicios mediante sistemas de crédito, el proveedor estará obligado a informarle en forma previa[29], clara y precisa:

1. El precio al contado del bien o servicio materia de la transacción30;
2. El monto total correspondiente a intereses, la tasa a la que serán calculados31; así como la tasa de interés moratoria y todos los demás recargos adicionales;
3. El número, monto y periodicidad de los pagos a efectuar; y,
4. La suma total a pagar por el referido bien o servicio.

---

27 Ley Orgánica de Defensa del Consumidor.

28 Aunque el "orden público" pudiera traducirse cualquier estipulación en contra de norma prohibitiva, las "buenas costumbres" es una categoría de mayor ambigüedad sobre la que se a escrito sin consenso. Nótese que una cláusula que vaya contra el "orden público" con el alcance aquí señalado llevaría a una nulidad no subsanable del contrato (nulidad absoluta), aunque por la disposición le agravaría a la de la nulidad de pleno derecho.

29 Hay que distinguir, en tratándose de la contratación en modalidad *webpage*, si el oferente otorga crédito propio o la compra se hace con tarjeta de crédito. En el primer caso, la obligación estará cumplida con la información al momento de la calificación como sujeto de crédito, que en todo caso un link al respecto puede direccionar al usuario visitante. En el segundo, el contrato de emisión de tarjeta de crédito establece el costo del crédito.

30 El precio suele estar en la imagen del producto y en la cuenta del carrito de compras, previo al *check in*. En caso de servicios, menos frecuente, un tarifario en la misma *webpage* es común.

31 El algunos casos, un calculador del crédito puede encontrarse. Los intereses no pueden superar a los legales.

Se prohíbe el establecimiento y cobro de intereses sobre intereses[32]. El cálculo de los intereses en las compras a crédito debe hacerse exclusivamente sobre el saldo de capital impago. Es decir, cada vez que se cancele una cuota, el interés debe ser recalculado para evitar que se cobre sobre el total del capital. Lo dispuesto en este artículo y en especial en este inciso, incluye a las instituciones del sistema financiero.

1.7 En relación a la oportunidad del pago debido, la DECONSU, Art. 48 (1) [Pago anticipado], prescribe:

En toda venta o prestación de servicios de crédito, el consumidor siempre tendrá derecho a pagar anticipadamente[33] la totalidad de lo adeudado, o a realizar pre-pagos parciales en cantidades mayores a una cuota. En estos casos, los intereses se pagarán únicamente sobre el saldo pendiente.

2. Perfil de la aceptación

La plataforma internet que contiene la oferta busca la aceptación pura y simple (contrato de adhesión) a través de la aceptación, principalmente en la modalidad *web-page*.

Efectivamente, por un lado, los términos y condiciones (cláusulas predispuestas), incluyendo costos de envío, se encuentran a disposición del usuario, de tal manera que su aceptación se (presupone) a través del *click* correspondiente[34]; y, por otro lado, no hay lugar a una contraoferta[35], ya que la arquitectura del sitio no abre la posibilidad de negociación adicional a la establecida[36]. De esta forma, una contratación de formación simultánea es identificable.

En caso de que el contrato sea realizado por la modalidad *on line* –a través de un sitio *web*-, se entenderá por perfeccionado cuando el comprador llene el for-

---

32 El anatocismo está prohibido por el Código Civil. "Art. 2113.- Se prohíbe estipular intereses sobre intereses".

33 Lo cual implica una modificación al principio general clásico del contrato de préstamo de consumo del Código Civil. "Art. 2107.- Podrá el mutuario pagar toda la cantidad prestada, aún antes del término estipulado, salvo que se hayan pactado intereses". Es un caso de modificación unilateral del contrato por parte del mutuario.

34 La técnica de aceptación puede variar desde un simple *click*-aceptación de los términos y condiciones hasta un *brosewrap* en un *link* de descarga del *software*.

35 Aunque el Art. 146 CComercio instrumenta la teoría *mirror image* en el sentido que la "aceptación condicional" es una verdadera contraoferta, la plataforma internet no da pie a su existencia. En sentido contrario § 2-207 *Uniform Commercial Code* admite aceptación incluyendo términos no esenciales de la oferta.

36 Salvo que se haga uso de manera desnaturalizada el espacio de "requerimientos especiales" del envío como un foro que el usuario invite al proveedor a una negociación sobre los términos y condiciones.

mulario predeterminado y manifieste su voluntad haciendo un click en el ícono de aceptar la compra; el vendedor debe, por su parte, enviar un mensaje referente a dicha operación. (Varennes et al, 2005, p. 75)

Situación diversa ocurre si la modalidad de negociación es vía *email*, en la que se abre la posibilidad de una cadena de contraofertas y nuevas ofertas, que ciertamente las ubican en tratativas preliminares. En esta hipótesis, una contratación de formación sucesiva es reconocida.

Así mismo, la contratación a través de plataforma internet elimina el fenómeno largamente discutido del momento de la aceptación de la contratación por correspondencia[37] ("Por todas las razones expuestas, creemos que la doctrina seguida por el Código es la sentada por el artículo [...], es decir, la de la EXPEDICIÓN, con algunas atenuaciones [...]" Sapena, 1944, p. 79), ya que el tratamiento que debe darse a la negociación es la de una entre partes presentes (presencia virtual), aunque la oferta es a persona indeterminada.

Así, la COMELEC, en el Art. 46 (1) [Perfeccionamiento y aceptación de los contratos electrónicos], preceptúa:

El perfeccionamiento de los contratos electrónicos se someterá a los requisitos y solemnidades[38] previstas en las leyes y se tendrá como lugar de perfeccionamiento el que acordaren las partes.

En todo caso, el lugar de perfeccionamiento del contrato se entenderá en el del aceptante (*locus regit actum*), que es la solución que trae nuestra norma mercantil[39] para el caso de contratación por correspondencia.

En resumen: respecto al momento y lugar del nacimiento del contrato a través de plataforma internet se reconoce que

La rapidez en el intercambio electrónico de datos característica de la tecnología de la sociedad de la información tiende a reducir la importancia de la referida disparidad de soluciones en la medida que facilita la simultaneidad de las comu-

---

37 Teoría de la simple aceptación, teoría de la expedición, teoría de la recepción, teoría dual de Windscheid. El Art. 142 CComercio se inclina por una plazo legal en el sentido que la aceptación debe hacerse dentro de las 24 horas de recibida la oferta y, residiendo las partes en diferente plaza, a vuelta del primer correo después de las 24 horas de recibida la oferta.

38 Los contratos solemnes son los prescritos por la ley, a saber: compraventa, permuta, aporte y donación inmobiliaria y cualquier obligación de transferencia de derecho real sobre inmuebles, incluyendo fijación de linderos, fraccionamiento e integración inmobiliaria, contrato de compañía mercantil, contrato de fideicomiso. Por lo mismo, no encontramos razón de ser para la disposición respecto a la contratación electrónica.

39 CComercio, "Art. 147.- Residiendo las partes contratantes en distintos lugares, se entenderá celebrado el contrato, para todos los efectos legales, en el de la residencia del que hubiere aceptado la propuesta primitiva o la propuesta modificada".

nicaciones, marco en el que el carácter instantáneo y de sucesivo de la formación del contrato provoca que la determinación del momento de la celebración se plantee en los términos típicos de la contratación entre presentes. [DE MIGUEL, 2002, p.363]

3. Presunciones legales

Finalmente, la COMELEC, en su Art. 11 [Envío y recepción de los mensajes de datos], prescribe:

Salvo pacto en contrario, se presumirá que el tiempo y lugar de emisión y recepción del mensaje de datos, son los siguientes:

a) Momento de emisión del mensaje de datos.- Cuando el mensaje de datos ingrese en un sistema de información o red electrónica que no esté bajo control del emisor o de la persona que envió el mensaje en nombre de éste o del dispositivo electrónico autorizado para el efecto;

b) Momento de recepción del mensaje de datos.- Cuando el mensaje de datos ingrese al sistema de información o red electrónica señalado por el destinatario. Si el destinatario designa otro sistema de información o red electrónica, el momento de recepción se presumirá aquel en que se produzca la recuperación del mensaje de datos. De no haberse señalado un lugar preciso de recepción, se entenderá que ésta ocurre cuando el mensaje de datos ingresa a un sistema de información o red electrónica del destinatario, independientemente de haberse recuperado o no el mensaje de datos; y,

c) Lugares de envío y recepción[40]. Los acordados por las partes, sus domicilios legales o los que consten en el certificado de firma electrónica, del emisor y del destinatario. Si no se los pudiera establecer por estos medios, se tendrá por tales, el lugar de trabajo, o donde se desarrollen el giro principal de sus actividades o la actividad relacionada con el mensaje de datos.

Debe entenderse como presunciones que admiten prueba en contrario.

II. Autenticidad y Prueba del Contrato

Aunque el régimen aplicable a la contratación a través de plataforma internet es la misma que una entre presentes, dos cuestiones particulares aparecen como consecuencia del uso tecnológico. La primera referente a la certidumbre de los sujetos y, la segunda, sobre el alcance del acuerdo.

4. Autenticidad de la voluntad

Un acto tienen el carácter de auténtico cuando tiene un autor cierto, identifica-

40 Entendemos que se trata de la determinación para el cumplimiento de las prestaciones o eventuales reclamos judiciales.

ble, de tal manera que le sea imputable el contenido de la voluntad.

El fenómeno en la contratación a través de plataforma internet radica así mismo en identificar a la fuente de la voluntad, al sujeto contractual.

La COMELEC, en el Art. 2 [Reconocimiento jurídico de los mensajes de datos], prescribe:

Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterán al cumplimiento de lo establecido en esta Ley y su Reglamento.

Aunque la norma parecería trabajar sobre una correspondencia electrónica, el caso de contratación a través de una *webpage* no se excluye. La identificación de la interfaz en red (*ip*), el alojamiento (*hosting*)("[…] instalar sus propias aplicaciones informáticas y contenidos en los componentes de hardware y software de la otra parte", ÉCIJA, 2002, p. 133), suministro de *cookies*, etcétera, son recursos que viabilizan la identificación de los contratantes.

Iniciador es la persona física o jurídica que envía o genera un mensaje de datos. Su actividad puede por tanto consistir en una o dos conductas conceptualmente distintas: la generación y/o el envío de un mensaje de datos. Por generación debe entenderse tanto la redacción del mensaje de datos previa a su envío –siendo el envío efectuado posteriormente por persona distinta a la de quien lo genera- cuanto la redacción automática de un mensaje de datos por medio de un agente electrónico sometido al control del iniciador. En envío de un mensaje de datos, por el contrario, consiste en la actividad electrónica necesaria –impulso o pulse electrónico como mínimo- para proceder a la expedición del mismo hacia su destinatario lo que positivamente se ha de producir cuando el mensaje de datos «entre en un sistema de información que no esté bajo control del iniciador o de la persona que envío el mensaje de datos en nombre del iniciador» [Illescas, 2001, p. 118]

En relación, el Art. 10 [Procedencia e identidad de un mensaje de datos] *ibídem*, prescribe:

Salvo prueba en contrario se entenderá que un mensaje de datos proviene de quien lo envía y, autoriza a quien lo recibe, para actuar conforme al contenido del mismo, cuando de su verificación exista concordancia entre la identificación del emisor y su firma electrónica, excepto en los siguientes casos:

a) Si se hubiere dado aviso que el mensaje de datos no proviene de quien consta como emisor; en este caso, el aviso se lo hará antes de que la persona que lo recibe actúe conforme a dicho mensaje. En caso contrario, quien conste como emisor deberá justificar plenamente que el mensaje de datos no se inició por orden suya o que el mismo fue alterado; y,

b) Si el destinatario no hubiere efectuado diligentemente las verificaciones correspondientes o hizo caso omiso de su resultado.

A diferencia, la autenticación no requiere de firma electrónica[41] alguna sino por el hecho de identificar tecnológicamente[42] al presunto oferente o aceptante, tratándose de correspondencia electrónica. En el caso de *webpage*, una identificación interna de usuario (membresía) o, en el caso de usuario visitante, la provisión de la forma de pago, presupone autenticidad de aceptación.

5. Autenticidad del alcance del contrato

Un acto contiene autenticidad de contenido en el momento que se genera prueba del mismo.

La COMELEC, en el Art. 45 [Validez de los contratos], prescribe:

> Los contratos podrán ser instrumentados mediante mensajes de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos.
>
> Lo anterior, reconoce la instrumentalización electrónica de los contenidos. A su vez, la COMELEC en el Art. 7 [Información original], prescribe:
>
> Cuando la ley requiera u obligue que la información sea presentada o conservada en su forma original, este requisito quedará cumplido con un mensaje de datos, si siendo requerido conforme a la Ley, puede comprobarse que ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos.
>
> Se considera que un mensaje de datos permanece íntegro, si se mantiene completo e inalterable su contenido, salvo algún cambio de forma, propio del proceso de comunicación, archivo o presentación.
>
> Por acuerdo de las partes y cumpliendo con todas las obligaciones previstas en esta Ley, se podrán desmaterializar los documentos que por ley[43] deban ser instrumentados físicamente.

---

41 La COMELEC en varias normas el régimen parecería dar valor de autenticidad del autor en la medida en que se manifieste con firma electrónica.

42 COMELEC, Art. 47 [Jurisdicción] (2): "Para la identificación de la procedencia de un mensaje de datos, se utilizarán los medios tecnológicos disponibles, y se aplicarán las disposiciones señaladas en esta Ley y demás normas legales aplicables".

43 Salvo para el caso de prueba instrumental, la ley no establece la obligatoriedad de prueba instrumental privada, salvo el caso de algunas modalidades de contrato individual de trabajo. Esta misma concepción se reproduce en el Art. 41 COMELEC [Información escrita] "Cuando la ley requiera u obligue que la información conste por escrito, este requisito quedará cumplido con un mensaje de datos, siempre que la información que éste contenga sea accesible para su posterior consulta".

Los documentos desmaterializados deberán contener las firmas electrónicas[44] correspondientes debidamente certificadas ante una de las entidades autorizadas según lo dispuesto en el artículo 29 de la presente Ley, y deberán ser conservados conforme a lo establecido en el artículo siguiente.

Por lo mismo, aunque el contenido se manifiesta electrónicamente, la susceptibilidad de ser reducido a escrito es reconocida, con el mismo valor jurídico del mensaje original.

III. Acciones frente al Incumplimiento

Sin perjuicio del derecho alternativo por parte del vendedor frente a la mora en el cumplimiento contemplados en la ley sustantiva civil y mercantil (acción de cumplimiento o acción de resolución, con indemnización por daños y perjuicios en cualquiera de los casos), y las acciones de saneamiento por evicción, por vicio redhibitorio o *quanti minoris*, la DECONSU ha establecido un repertorio de remedios de subsanación, administrativos, civiles y penales.

En primer lugar, debemos distinguir en materia de ejecución contractual, los contratos electrónicos *directos* frente a los contratos electrónicos *indirectos*. En los primeros la satisfacción del interés del adquirente del bien o servicio se produce a través de un terminal (sea un ordenador, un teléfono, televisión interactiva, etc). Se trata de adquirir bienes inmateriales, producto del intelecto del autor, y que pueden ser objeto de copia por el adquirente mediante un procedimiento electrónico consistente en descargar el bien desde la web en la que es ofrecido. [...] No hay temor a un retraso en la entrega, o a que el bien recibido sea defectuoso –aunque si cabría, en teoría, una manipulación indebida del pago del precio-, tampoco parece que quepa opción al desistimiento o arrepentimiento cuando el adquirente goza plenamente del bien adquirido y pude disfrutar de la música o de la obra literaria o información, [...]. En cambio, en el comercio electrónico indirecto, las partes celebran un contrato en que las prestaciones deben ejecutarse fuera de la red. [Fernández, p. 179]

6. Derecho de devolución de la cosa

La DECONSU, en el Art. 45 [Derecho de devolución[45]], prescribe:

El consumidor que adquiera bienes o servicios por teléfono, catálogo, televisión, internet o a domicilio, gozará del derecho de devolución, el mismo que deberá

44 Una vez más, parecería que la eficacia de la materialización depende de la existencia de firma electrónica cuando por otros medios pudiera alcanzarse la autenticidad de autor.

45 La DECONSU, en el Art. 2 [Definiciones], a propósito del término “Derecho de Devolución”, condiciona la facultad “siempre que la venta del bien o servicio no haya sido hecha directamente, sino por correo, catálogo, teléfono, internet, u otros medios similares”. Es decir, no fue a la vista y, por lo mismo, no tuvo derecho de examen.

ser ejercido dentro de los tres días posteriores a la recepción del bien o servicio, siempre y cuando lo permita su naturaleza[46] y el estado del bien sea el mismo en el que lo recibió[47]. En el caso de servicios, el derecho de devolución se ejercerá mediante la cesación inmediata del contrato de provisión del servicio.

Este derecho presupone una condición resolutoria del contrato, potestativa del acreedor (consumidor), a dejar sin efecto el mismo. Es una vía expedita para alcanzar el régimen de prestaciones mutuas.

De allí la necesidad de establecer en los contratos informáticos la diferenciación entre la recepción y la aceptación del producto o servicio contratados y definir claramente en qué consistirá el test de aceptación que debe ser cumplido para que la recepción se convierta en entrega aceptada. [Martorrel, 2002, p.663]

7. Derecho de reparación, reposición, devolución del precio e indemnización

La DECONSU, en el Art. 71 [Indemnización, reparación, reposición y devolución], prescribe:

Los consumidores tendrán derecho, además de la indemnización por daños y perjuicios ocasionados[48], a la reparación gratuita del bien y, cuando no sea posible, a su reposición o a la devolución de la cantidad pagada[49], en un plazo no superior a treinta días, en los siguientes casos:

1° Cuando en el producto que se hubiere adquirido con determinada garantía y, dentro del plazo de ella, se pusiere de manifiesto la deficiencia o características del bien garantizado, siempre que se hubiere destinado al uso o consumo normal de acuerdo a la naturaleza de dicho bien[50]. Este derecho ejercerá siempre y cuando el proveedor haya incumplido con la garantía;

2° Cuando cualquier producto, por sus deficiencias de fabricación, elaboración, estructura, calidad o condiciones sanitarias, en su caso, no sea apto para el uso al cual está destinado; y,

3° Cuando considerados los límites de tolerancia permitidos, el contenido neto

---

46 Excluiría a bienes o servicios consumibles, incluyendo un programa visual exclusivo, a verificarse en una fecha.

47 Salvo el desgaste natural por el uso ordinario, como aplicación de las reglas de la restitución.

48 Aquí se abre una discusión sobre si la indemnización debe satisfacer, a más del daño emergente, el lucro cesante. La indemnización por daño moral en estos casos también es un tema relevante. En todo caso, debe existir prueba de causalidad y del monto del daño.

49 Aunque no hay discusión que en esta alternativa corresponde a la cantidad pagada, sí pudiera existir respecto a si debe incluir los intereses correspondientes desde su exigibilidad o, acaso éstos, se reconocen como indemnización.

50 En todo caso es susceptible de apreciación de perito.

de un producto resulte inferior al que debiera ser o la cantidad sea menor a la indicada en el envase o empaque.

Sin perjuicio de las acciones civiles, penales o administrativas a que hubiere lugar, el proveedor que incurriere en uno de los casos contemplados en este artículo, e incumpliere su obligación una vez fenecido el plazo establecido, será sancionado con una multa equivalente al valor del bien o servicio[51], que en ningún caso será inferior a ciento veinte dólares de los Estados Unidos de América o su equivalente en moneda de curso legal, sin que ello extinga su obligación de reparar o reponer el bien, o en su caso restituir lo pagado.

Este derecho tiene carácter alternativo, adicional a la indemnización por los daños y perjuicios que el bien o el servicio ocasione. En relación a la devolución de la cantidad pagada, no es otra cosa que el reflejo a la devolución de la cosa.

8. Sanciones administrativas

La DECONSU, a su turno, también prescribe sanciones administrativas, con multa, a saber: Art. 72 en caso de publicidad engañosa o abusiva del proveedor, sanción de rectificación de la publicidad más multa; Art. 73 en caso de no restitución del valor del bien de un servicio, sanción con clausura provisional o definitiva; Art. 74 en caso de constatación de daño en un producto peligroso o riesgoso, multa; Art. 77 en caso de suspensión injustificada de un servicio, con multa.

9. Competencia

La DECONSU establece dos niveles de competencia: la Defensoría del Pueblo y EL Juez de Contravenciones.

El Defensor Público es competente para conocer los reclamos y quejas por inobservancia de los derechos fundamentales del consumidor en procedimiento abreviado que se circunscribe a un informe que podrá ser apreciado por el juez.

El Juez de Contravenciones es competente para conocer denuncias por cometimiento de infracciones a la DECONSU, en procedimiento oral circunscrito a la audiencia de juzgamiento. La resolución es susceptible de apelación al Juez Penal. Curiosamente el procedimiento tiene como primer nivel de juzgamiento una autoridad administrativa y, en segundo, una autoridad de derecho.

10. Pago del precio

El pago del precio por el bien o el servicio también dependerá de la modalidad

---

51 Independientemente al estado del bien o servicio proveído, la sanción pecuniaria corresponde al valor total de la cosa.

contractual. Así, eCommerce puede reconocer un pago con una parrilla de pagos, incluyendo crédito propio o pago contra-entrega, a opción del consumidor.

Existen diferentes tipos de pagos electrónicos.

Monedero electrónico: lo que se maneja es dinero electrónico almacenado en una tarjeta inteligente o como fichero en el disco de un ordenador, se basa en un sistema de prepago, esto es, se obtienen a cambio de dinero real. Se basan en "tokens" /secuencias de bits que representan un cierto valor en sí mismas); para certificar su valor, el banco emisor los firma con su firma digital y lo carga en la cuenta del usuario. Es característico de los micropagos y su desventaja es que en caso de sustracción no hay posibilidad de impedir su gasto (como nuestros billetes y monederos). Si el comercio es de empresa a consumidor, el procedimiento es muy similar al pago con tarjeta de crédito, es el "protocolo SET" (Secure Electronic Transaction) que utiliza procedimientos de cifrado simétrico y asimétrico, firmas digitales y certificados. Finalmente si el comercio es entre empresas, sobre todo PYMES, el pago suele ser mediante cheques electrónicos como e-Check o Netcheque. Si el comercio es de empresa a consumidor, el procedimiento es muy similar al pago con tarjeta de crédito, es el "protocolo SET " (Secure Electronic Transaction) que utiliza procedimientos de cifrado simétrico y asimétrico, firmas digitales y certificados. Finalmente si el comercio es entre empresas, sobre todo PYMES, el pago suele ser mediante cheques electrónicos como e-Check o Netcheque. [Martínez, 2003, p. 13]

IV. Modalidad eCommerce

La contratación electrónica se ha desarrollado a través de una *webpage* personalizada por cada empresa comercial. De esta forma, el portal se convierte en el centro de publicidad de la marca, tendencias, fidelidad (club de fans y sistema de puntos), compras, etcétera.

La descripción anterior *.com*, junto con el *social media marketing*, constituyen la base del comercio vinculado a la tienda virtual, con visitas y transacciones en tiempo presente entre B2C (*business to consumer*), B2B (*business to business*), C2C (*consumer to consumer*)[52].

La arquitectura tecnológica de recursos[53] del sitio puede sintetizarse así[54]:

52 No forma parte del trabajo las interacciones comerciales C2G (*consumer to government*), B2G (*business to government*), G2G (*government to government*).

53 Vulgarmente conocidos como "legales".

54 Aunque el trabajo se refiere a la contratación local, la recopilación de términos y condiciones ha sido hecha de los portales amazon.com, ebay.com, forever21.com, Apple.com, garmin.com, target.com, macys.com.

A. Condiciones de uso de software para venta:

1. Privacidad.
    a. Aviso de privacidad.
    b. Cookies y publicidad en internet.
2. Comunicaciones electrónicas.
3. Derechos de autor, derechos de propiedad intelectual y derechos sobre base de datos.
    a. Jurisdicción.
    b. Titularidad.
    c. Prohibiciones.
4. Marcas registradas.
    a. Lista.
    b. Prohibición de uso.
5. Patentes.
6. Licencia y acceso.
    a. Términos de licencia de acceso y utilización de servicios.
    b. Derechos del licenciatario.
    c. Obligaciones del licenciatario.
    d. Prohibiciones.
7. Su cuenta.
    a. Confidencialidad.
    b. Responsabilidad de acciones.
    c. Actualización de información.
    d. Políticas y prohibiciones de uso.
8. Opiniones, comentarios, comunicaciones y otros.
    a. Contenido de las publicaciones.
        i. Propiedad intelectual.
    b. Obligaciones.

c. Prohibiciones.

9. Reclamaciones sobre propiedad intelectual.

a. Política y procedimiento de reclamaciones por infracción.

10. Condiciones generales sobre el software.

11. Otras páginas vinculadas.

12. La obligación del servidor.

13. Ley aplicable.

14. Modificación del servicio o variación de las condiciones.

15. Renuncia.

16. Menores de edad.

17. Procedimiento y formulario de aviso de vulneración de derechos.

18. Aviso relativo a las ofertas de venta.

19. Condiciones de uso adicionales del software.

a. Uso del software.

i. Propósitos.

ii. Inobservancia.

iii. Utilización de servicios de terceros.

B. Condiciones de venta:

1. Obligaciones del vendedor.

a. Confirmación.

b. Envío.

c. Constancia.

2. Derecho de desistimiento, excepciones al derecho de desistimiento, garantía de devolución voluntaria y garantía legal de conformidad.

a. Derecho y excepciones.

b. Procedimiento.

c. Efectos del desistimiento.

i. Reembolso del precio y gastos de envío.

d. Excepciones al derecho de desistimiento.

e. Garantía de devolución voluntaria.

i. Condiciones.

ii. Reembolso.

3. Precios y disponibilidad.

a. Política de precios.

4. Información del producto.

a. Contenidos.

b. Promociones.

5. Información aduanera.

6. Comentarios de los usuarios, retroalimentación, cartas postales y otros.

7. Privacidad.

8. Terminación.

a. Formas de terminación.

9. Modalidades de compra.

a. Pedidos en 1-click.

b. Pedidos comunes.

10. Límites de responsabilidad.

a. Pérdidas no atribuibles al cumplimiento del vendedor.

b. Pérdidas empresariales.

c. Pérdidas indirectas.

d. Demoras.

e. Garantía de conformidad.

11. Ley aplicable.
12. Jurisdicción.
13. Modificación de condiciones de venta.

a. Facultad de realizar cambios en sitio web, políticas o términos y condiciones.

14. Renuncia.
15. Menores de edad.

Ciertamente, las políticas del uso y los términos y condiciones de visualización y contratación no pudieran orillar la ley local tratándose de un oferente domiciliado en territorio nacional. Es materia de otro estudio el conflicto de leyes en tratándose de un oferente con domicilio fuera de territorio local o sin domicilio físico.

V. Conclusión

El régimen directo e indirecto (subsidiario) de contratación electrónica instrumenta los principios generales de la obligación contractual, más todavía cuando la regulación de defensa y protección del consumidor puede considerarse sobre el *standard*. Sin embargo, especial atención debe tenerse en la presunción de aceptación por la estructura de cada una de las webpages.

Bibliografía:

Brizzio C. (2001). Regulación del Contrato en la Economía Globalizada. Revista de Doctrina, 3, 55.

De Miguel, P. (2002). Derecho Privado de Internet. Madrid: Civitas.

Écija, A. (2002). Contratos de Internet (Modelos y Comentarios Prácticos). Navarra: Arazandi.

Fernández, R. El cumplimiento del contrato celebrado en internet: especialidades. 12 Octubre 2016, de V/LEX España Sitio web: http://libros-revistas-derecho.vlex.es/vid/cumplimiento-contrato-especialidades-417359722.

Illescas, R. (2001). Derecho de la Contratación Electrónica. Madrid: Civitas.

Martínez, M. (2003). El contrato electrónico y sus elementos esenciales. 12 Octubre 2016, de Saberes UAX Sitio web: http://www.uax.es/publicacion/el-contrato-electronico-y-sus-elementos-esenciales.pdf.

Martorrel, E. (2002). Tratado de los Contratos de Empresa, Tomo III. Buenos Aires: Depalma.

Pardo Gato, J. (2003). Las páginas Web como soporte de condiciones generales contractuales. Navarra: Arazandi.

Rivero Alemán, S. (2002). Crédito, Consumo y Comercio Electrónico (Aspectos Jurídicos Bancarios). Navarra: Arazandi.

Sapena Pástor, R. (1944). Los contratos por correspondencia (en el Código Civil argentino y en el derecho internacional privado). Buenos Aires: Imprenta López.

Varennes F. & Rey, C. (2005). E-commerce. I-commerce. En Contrataciones Empresarias.

SEGUNDA PARTE

PONENCIAS DE LA SOCIEDAD CIVIL

El acceso a internet: habilitador del ejercicio de derechos humanos

Valeria Betancourt
Directora del Programa de Políticas de Información y Comunicación de Asociación para el Progreso de las Comunicaciones (APC)

Es incuestionable que el acceso a internet, más allá de contribuir a los procesos de desarrollo y a los esfuerzos por lograr la justicia social, amplía las posibilidades de los individuos y colectivos de disfrutar la realización plena de sus derechos. El ex Relator especial de Naciones Unidas, Frank La Rue, señala lo siguiente, acerca de la promoción y protección del derecho a la libertad de opinión y expresión: "Internet es uno de los instrumentos más poderosos del siglo XXI para incrementar la transparencia en la conducta de quienes ejercen el poder, acceder a la información y facilitar la participación ciudadana activa en la construcción de sociedades democráticas" (La Rue, 2011, p. 1).

La relación entre el acceso a internet y los derechos humanos debe analizarse desde dos ángulos: uno, la provisión del acceso como instrumento que habilita el ejercicio y el disfrute de los derechos humanos y, dos, por su parte, los derechos humanos como marco que habilita una buena gobernanza que resulta en políticas públicas orientadas a un acceso universal, asequible y de calidad.

Contar con un acceso universal, asequible y de calidad no es el único desafío. Una vez que el acceso ha sido provisto, es preciso que pueda ser usado por las personas de manera libre y segura, si es que va a ser utilizado en función de transformar sus vidas y las condiciones que las determinan. Esto se trata de ideales cuya realización está aún lejos de ser lograda. La brecha digital nunca ha sido tan grande como en la actualidad. Así como nunca ha sido tan creciente la tendencia de los gobiernos y de las corporaciones a ejercer control desmesurado sobre la red, su infraestructura, sus servicios, aplicaciones y contenidos.

Las violaciones y restricciones a los derechos humanos relacionadas con la tecnología son una manifestación de las violaciones de derechos fuera de internet. Al mismo tiempo, las inequidades en el acceso a internet devienen en nuevas formas de discriminación, marginación y desequilibrios de poder y también en la perpetuación de situaciones de discriminación estructural relativas al entorno fuera de línea.

1. Los desafíos actuales en torno al acceso

Para abordar efectivamente las desigualdades en el acceso, se debe mirar más allá de las tasas de penetración. La categorización de 'conectado' y 'no conectado' resulta limitada para reflejar el hecho de que "existe un amplio espectro de niveles de conectividad que van desde la desconexión completa hasta las conexiones sin límite a la gran banda ancha, con la mayoría de las personas en un lugar intermedio, prevaleciendo las conexiones irregulares mediante enlaces de banda ancha móviles, que son costosos, de baja velocidad y con medidor de tráfico" (APC, 2016, p. 2).

Si se desagregan los datos de los grupos menos favorecidos (en particular el de las mujeres), las desigualdades en el acceso se hacen aún más notorias. La reducción y la eliminación de la exclusión digital demanda de un incremento en la cobertura a bajo costo de los servicios de banda ancha móvil y fijos. Demanda, además, estimular el desarrollo de las capacidades técnicas y humanas y de las herramientas para solventar las necesidades de conectividad en los niveles locales[1] a través de, por ejemplo, el despliegue de redes autónomas comunitarias[2] para usar efectivamente las aplicaciones y el contenido.

El costo del acceso a internet es un limitante importante en entornos de mercado con nula o poca competencia. La escasa distribución de infraestructura básica de telecomunicaciones y el acceso limitado al uso de las frecuencias del espectro

---

1 En términos de ciberseguridad, la habilidad de las personas y comunidades de instalar y manejar sus propias redes les da, por ejemplo, el poder de hacerlo en los intereses públicos y basados en el respeto y en la defensa de los derechos humanos, reduciendo el impacto del creciente control gubernamental y corporativo sobre la infraestructura, los contenidos y los usuarios.

2 Altermundi ofrece un modelo de baja complejidad y de bajo costo para la instalación, despliegue y operación de redes libres comunitarias. http://docs.altermundi.net/RedComunitaria/.

radioeléctrico agravan aún más la posibilidad de ofrecer conectividad de calidad y de bajo costo en el contexto de los países en desarrollo.

La implementación de políticas públicas de acceso debe apuntar no solo a conectar a los que no están conectados, sino también a mejorar la conectividad de los que están conectados, pero restringidos en el uso de internet, debido a bajas velocidades de conexión, altos costos de servicios de banda ancha y acceso limitado a contenidos y aplicaciones a causa de estrategias de tasa cero (*zero-rating*).

Las políticas públicas deben apuntar también a incrementar y mejorar las facilidades de acceso público en bibliotecas, infocentros o telecentros y centros comunitarios multipropósito. Y, partiendo del hecho de que las políticas son interdependientes, se deben atender los factores que indirectamente inciden en el acceso a internet como la provisión de energía eléctrica, la alfabetización digital, la existencia de aplicaciones y contenidos locales, los impuestos a servicios de tecnología, entre otros.

Conviene poner énfasis en las estrategias de infraestructura compartida, cuyos beneficios suelen desestimarse. Un estudio realizado recientemente por APC, que busca sensibilizar sobre los beneficios de las políticas de infraestructura compartida en los planes nacionales de banda ancha en países en desarrollo (APC, 2015), reveló que el ahorro en países en desarrollo asciende a miles de millones, si comparten infraestructura como un mecanismo para acelerar el acceso universal a banda ancha.[3]

En definitiva, la solución no pasa por enfocarse exclusivamente en la infraestructura. Los esfuerzos e iniciativas de despliegue y mejora de infraestructura deben estar acompañados de esfuerzos para derribar las barreras políticas, económicas, sociales y culturales que frenan el acceso pleno a internet. Solamente de esa manera, el internet podrá contribuir al desarrollo humano, social y económico.

2. Las amenazas más apremiantes a los derechos en línea

Un acceso a internet limitado, controlado y filtrado no es un acceso real. Las amenazas más apremiantes no tienen que ver solo con el bloqueo y con la censura de contenidos, con la interferencia en la privacidad mediante la vigilancia masiva, con el usufructo comercial y político de los datos personales, con el acceso a datos de geolocalización sin orden judicial o con la retención obligatoria de datos. Las amenazas están también relacionadas con la radicalización de la aplicación de leyes de derecho de autor como mecanismo para silenciar voces críticas, la violación a la neutralidad de la red con el propósito de privilegiar ciertas aplicaciones y contenidos a partir de prácticas de mercado y modelos de negocio como las de tasa cero, el atentado contra una internet libre y abierta con la adopción de soluciones

3 El ahorro se logra compartiendo infraestructura de telecomunicaciones con la de otros servicios públicos, como red eléctrica, oleoductos, redes viales y férreas, entre otros.

privadas como el proyecto *Free Basics* de Facebook, la dilución de la pluralidad y la diversidad de actores y contenidos en línea, debido a la consolidación de formas de concentración y de propiedad cruzada de las plataformas de medios y servicios electrónicos, resultantes de la convergencia de tecnologías de radiodifusión y de banda ancha.[4]

La violencia contra la mujer basada en y mediada por la tecnología[5] es, incuestionablemente, uno de los problemas más complejos que resulta en la afectación de una serie de derechos humanos, "provoca daño psicológico y emocional, refuerza los prejuicios, afecta la reputación, causa daños económicos y coloca barreras para la participación en la vida pública" (LACNIC, 2015, p. 154).

Lo que incrementa los riesgos en el presente y en el futuro cercano es que los nuevos usuarios pueden no estar completamente conscientes de la histórica naturaleza abierta y libre de internet y de su importancia, simplemente debido a que su experiencia actual de acceso a internet está mediada por el filtrado de contenidos, los jardines amurallados, la privacidad comprometida y el minado de sus datos personales con fines de lucro.

A pesar de las recomendaciones que diversos Relatores Especiales de Naciones Unidas han emitido para gobiernos y corporaciones, sobre las resoluciones adoptadas en la Asamblea General de Naciones Unidas y en el Consejo de Derechos Humanos, acerca de los estándares producidos por la Comisión Inter Americana de Derechos Humanos, y los lineamientos que organizaciones de la sociedad civil han producido con la perspectiva de reforzar el ejercicio de derechos humanos en línea[6], queda aún mucho por hacer para que las políticas y la gobernanza de internet en los niveles globales, regionales y nacionales apunten a hacer prevalecer el interés público y garanticen el disfrute pleno de los derechos humanos dentro y fuera de línea.

Espacios como el Foro regional de América Latina y el Caribe sobre gobernanza de internet (*LAC IGF*)[7] ofrecen una oportunidad valiosa para discutir preocupaciones actuales como el impacto de los acuerdos comerciales interregionales en

---

4 Mike Jensen, de APC, ofrece una mirada actual sobre el fenómeno de la convergencia digital y las tendencias globales de la concentración de medios de radiodifusión y de banda ancha en http://www.apc.org/en/news/digital-convergence-global-trends-broadband-and-br.

5 Como por ejemplo el acoso y el chantaje en línea, la intromisión en la correspondencia y las comunicaciones privadas, la difusión no consentida de fotografías íntimas y la manipulación de imágenes con el propósito de afectar la reputación.

6 Un recuento de algunos informes principales, resoluciones y lineamientos se encuentra en la introducción del capítulo 'Internet para la promoción, garantía y ejercicio de los derechos humanos y libertades fundamentales' del libro por los 10 años del programa FRIDA disponible en http://lacnic.net/frida/FRIDA-book2015-es.pdf.

7 http://www.lacigf.org/sp/index.html

el acceso al conocimiento, las nuevas y crecientes capacidades de los actores gubernamentales y corporativos para la vigilancia y la falta de transparencia sobre objetivos y prácticas de vigilancia, el alcance y límite de las responsabilidades de los intermediarios de internet, los mecanismos para la reparación de los efectos de la afectación de derechos humanos en línea, los mecanismos de supervisión pública sobre la aplicación efectiva de la regulación de internet, entre otras. Ofrece también la posibilidad de ir avanzando en la configuración de una agenda regional de gobernanza de internet con la participación de los gobiernos, la sociedad civil, la comunidad técnica y el sector privado, en un ejercicio democrático de diálogo y colaboración sobre la base del modelo de múltiples actores interesados.

3. El riesgo de tornar el acceso a internet un asunto de seguridad nacional

El acceso a internet puede habilitar el desarrollo social y económico, incrementar y mejorar la participación de la sociedad civil en la esfera pública, facilitar la expresión de las voces marginadas y reforzar el disfrute de los derechos humanos. Sin embargo, el uso de internet con esos propósitos es frenado por la tendencia de convertir el acceso en un asunto de seguridad.

La necesidad de proteger la seguridad nacional es usada como argumento para ejercer un control excesivo sobre la infraestructura de la red y censurar contenidos en internet, perpetuando la falsa dicotomía de que la ciberseguridad solo puede garantizarse a expensas de la privacidad y otros derechos humanos.

Si bien el incremento en el acceso a internet ha resultado en un incremento de las amenazas como el cibercrimen, la respuesta no puede traducirse en un control desproporcionado del espacio en línea y en el escalamiento de los esfuerzos para militarizar el internet. La aplicación de políticas y estrategias de ciberseguridad se constituye en uno de los principales obstáculos para la realización de los derechos humanos en línea. Sin embargo, no es únicamente debido a la acción de los gobiernos. En su intento por maximizar los réditos, las corporaciones en el sector de tecnología están ejerciendo sus propias formas de control, no siempre evidentes para los usuarios. Un ejemplo de ello es la venta de tecnología y *software* para la ciberdefensa de varios gobiernos.

Es esencial que las iniciativas de ciberseguridad protejan la habilidad de acceder y usar el internet para el ejercicio de derechos humanos y para el desarrollo. El internet debe estar libre de vigilancia y violación de derechos humanos a nombre de la seguridad humana y nacional. Para que ello suceda, es fundamental reconocer y fortalecer el rol de la sociedad civil. Históricamente, el accionar y las propuestas de la sociedad civil han sido instrumentos para avanzar en las agendas de derechos humanos. La sociedad civil, incluyendo la academia, tiene un rol sumamente importante para abogar por la adopción de enfoques de derechos humanos en las

estrategias de ciberseguridad. La sociedad civil debe demandar la participación de los diversos actores en la formulación de políticas y acuerdos de acceso a internet y de ciberseguridad nacionales, regionales y globales.

Bibliografía:

Asociación para el Progreso de las Comunicaciones (APC). “Terminar con la exclusión digital: por qué persiste la brecha de acceso y cómo cerrarla”, APC <http://www.apc.org/en/system/files/APC_EndingDigitalExclusion_ES.pdf>. [04/2016].

Deloitte LLP for The Association for Progressive Communications (APC). “Unlocking broadband for all: Broadband infrastructure sharing policies and strategies in emerging markets”, Deloitte y APC

<http://www.apc.org/en/system/files/Unlocking%20broadband%20for%20all%20Full%20report.pdf>. [04/2015].

La Rue, F. (2011). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. United Nations document A/HRC/17/27.

Martínez, J.; y Robledo, L. (Editores). (2015) FRIDA 10 años contribuyendo al desarrollo de América Latina y el Caribe. Montevideo: LACNIC.

Limitaciones de la sociedad civil en la gobernanza de Internet en Ecuador: el caso del bloqueo de IPs por parte de los proveedores de Internet

Andrés Delgado-Ron
Co-Fundador del Colectivo Apertura Radical

1. Introducción

Según la definición emitida por la Cumbre Mundial sobre la Sociedad de la Información y avalada por la Resolución 56/183 de la Asamblea General de la ONU, entendemos como gobernanza de internet al “desarrollo y aplicación (…) de principios, normas, reglas, procedimientos de toma de decisiones y programas que den forma a la evolución y uso de Internet” en un formato multistakeholder. Decimos gobernanza y no gobierno porque este último término asume al Estado como único interlocutor válido de todos los sectores en un país. Gobernanza, implica la participación directa no solo de gobiernos, sino también del sector privado y de la sociedad civil. Sin embargo, las decisiones tomadas en diversos foros sobre gobernanza son meramente declarativos y dependen, en última instancia, de la voluntad de los gobiernos para ser adoptadas e implementadas.

Ecuador, desde 2007, ha adoptado una posición antagónica respecto al modelo multistakeholder en el plano internacional y, junto a países como Rusia y China, aboga por un modelo intergubernamental de gobierno de internet. Esta búsqueda por el monopolio en la toma de decisiones también se ve reflejada en la política interna. Las organizaciones de la sociedad civil están obligadas, mediante orden presidencial (Decreto Ejecutivo No.16, 2013), a alinearse a uno de los objetivos del plan de desarrollo y tienen prohibido involucrarse en actividades políticas "que atenten contra la seguridad interna" (Ortiz, 2014). Esto ya ha sido causal del cierre de organizaciones ambientales y, sobre la base de este decreto se ha amenazado a otras involucradas en la defensa del derecho a la libertad de expresión. Esta inseguridad jurídica, agravada por el requerimiento impuesto a las ONG de adherirse a un ministerio de gobierno (típicamente aquel al cual deben vigilar) ha ocasionado la inoperancia y, en ciertos casos, la inexistencia de ONG en el país.

Finalmente, la polarización de la política ecuatoriana genera dificultades en las organizaciones que deben trabajar pensando más allá de las ideologías. El momento en que las organizaciones toman posición respecto a un tema específico, tienden a ser clasificadas por los actores políticos y la opinión pública como parte de un "bando": el oficialismo o la oposición. Esto genera una estigmatización de las organizaciones que amenaza su capacidad de generar un diálogo adecuado en temas que usualmente ya son difíciles de explicar. Finalmente, este tipo de organizaciones de sociedad civil, al no involucrarse en la provisión de servicios, dependen casi siempre de donaciones por parte de actores privados internacionales, y eso, en el país, ha sido usado como una herramienta de deslegitimación por parte del poder ejecutivo.

El estado del tercer sector en la gobernanza de internet en Ecuador

El presente estudio busca analizar cómo las organizaciones de sociedad civil que trabajan en la defensa de derechos humanos en internet se han visto afectadas por las circunstancias descritas previamente. Para ello, se han seleccionado los casos (tres) más significativos de procesos relacionados con la gobernanza de internet en Ecuador, entre agosto de 2013 y julio de 2015, considerando su alcance nacional.

Eliminación del artículo 474 del Código Orgánico Integral Penal

La aprobación de un nuevo código penal en noviembre de 2013 motivó la formación del colectivo Internet Libre, el cual logró exitosamente eliminar el artículo 474 que, entre otras cosas, obligaba a que los usuarios sean filmados mientras usan Internet provisto por un tercero. Los intermediarios, dueños de cibercafés o particulares que usaban el teléfono o la computadora como "hotspots", (e incluso aquellos que proveían voluntariamente la clave de su señal wifi) debían guardar un registro de todas las páginas web visitadas por los usuarios durante un período mínimo de seis meses. Internet Libre, formado por una serie de organizaciones

privadas, públicas y del tercer sector (entes privados sin fines de lucro), logró exitosamente que la Asamblea Nacional derogue este articulado.

Primer Encuentro Nacional de Gobernanza de Internet

En noviembre de 2014 se realizó en CIESPAL el primer encuentro nacional de gobernanza de internet, cuya meta era proponer una agenda de gobernanza de internet en el país basándose "en el principio de interés público y en un enfoque de derechos humanos a través de un proceso participativo, abierto e inclusivo". Se realizó un análisis preliminar de la situación de Internet en Ecuador (Delgado, 2014) y se invitó a que expertos nacionales e internacionales discutan los resultados del mismo, vinculando a actores del Ministerio de Telecomunicaciones, Relaciones Exteriores y Asamblea Nacional.

Pronunciamiento en Defensa de la Privacidad en Ecuador

En julio de 2015 se filtraron una serie de documentos técnicos, económicos y administrativos de Hacking Team. Esta empresa, cuyo malware infecta computadoras, laptops y celulares con el fin de acceder a toda la información (almacenada en tiempo real), mantenía vínculos con la Secretaría de Inteligencia de Ecuador (Pérez, 2016). Algunos de los targets del software usado por esta empresa eran políticos y activistas (Leiva, 2016). En Ecuador, esto es ilegal e inconstitucional, lo cual motivó un fuerte pronunciamiento por parte de la sociedad civil. Varias organizaciones y colectivos se adhirieron a este petitorio, pero ninguno de los ocho puntos fueron acogidos por el gobierno central.

Se realizó una compilación de las organizaciones que han participado en al menos dos de estos escenarios que son exclusivamente de origen nacional. La pertenencia a los sectores empresarial o estatal fue utilizada como un criterio excluyente. La muestra resultante está descrita en la tabla 1.

Organizaciones del tercer sector involucradas en la gobernanza de Internet en Ecuador	**Personalidad Jurídica**	**Actividad Principal**
Apertura Radical	No	DDHH en internet
Asociación Radialistas Apasionadas y Apasionados	Sí	Democratización de comunicación
Asociación de Software Libre del Ecuador	Sí	Promoción de software libre
Asociación de Usuarios Digitales de Ecuador	No	DDHH en internet
Colectivo Central Dogma	No	Cultura abierta
Creative Commons Ecuador	No	Licenciamiento
Red Infodesarrollo (corporación mixta)	Sí	Reducción de brechas digitales

Tabla 1. Organizaciones de sociedad civil involucradas en actividades de defensa de derechos humanos en Internet (agosto 2013 - julio 2015). Elaboración: autor.

De todas las organizaciones involucradas en la gobernanza de internet, solamente Apertura Radical y la Asociación de Usuarios Digitales del Ecuador se dedican principalmente a la defensa de derechos humanos en Internet. En el período de estudio, ambas carecían de una figura jurídica y eran principalmente una presencia en la red. Tras dos años de iniciado el proceso, a Usuarios Digitales finalmente se le otorgó su personalidad jurídica, en agosto de 2015, mediante Acuerdo Ministerial (No. 034-2015, 2015). En este mismo documento se le prohíbe expresamente a la Asociación de Usuarios Digitales del Ecuador "intervenir en asuntos de carácter lucrativo, político o religioso", énfasis propio.

En la región, casi todos los países cuentan con al menos una organización de sociedad civil (constituida jurídicamente) que se dedica a la defensa de derechos humanos en la red. Existen organizaciones internacionales que brindan apoyo financiero y técnico a estas instituciones, lo que les ha ayudado a florecer en todo el continente, excepto en cuatro países: Venezuela, Bolivia, Ecuador y Uruguay. Este último es el único reconocido por la Unidad de Inteligencia de The Economist como una democracia completa o "full democracy" en América Latina (Unit, E. I., 2015), por lo cual, la ausencia de una organización fuerte de sociedad civil puede resultar menos preocupante; sin embargo, se requieren más estudios al respecto. Los otros tres países (Venezuela, Ecuador y Bolivia) tienen gobiernos con una ideología política socialista dominada por un fuerte poder ejecutivo, lo que sugiere una especie de correlación que merece ser estudiada.

Alcance del tercer sector en la gobernanza de internet en Ecuador

Como se mencionó en secciones previas, el decreto presidencial 16 (y su sustituto, el 739) obstaculizan el normal funcionamiento del tercer sector, al menos como este es entendido en su definición clásica (Stone, D. en Levi-Faur, D. & Oxford Handbooks Online Political Science, 2012). La prohibición de involucrarse en asuntos de carácter lucrativo o político influye decididamente en su financiamiento y desempeño. Esto se evidencia tanto en la ausencia de ONG (con personería jurídica, que defienden derechos digitales), como en la ausencia de estrategias que requieren coordinación para su ejecución, como es el caso de litigación de impacto o desarrollo sostenido de herramientas web. En cambio, funcionan, sobre todo, a base de campañas de educación y mediante la realización de propuestas específicas ("fiscalice", "derogue", "establezca", "exija", "cree") dirigidas al Estado en su papel de garante de derechos. Para ello, existen redes epistemológicas informales en las que expertos en ley, política pública y tecnología colaboran pro bono en forma esporádica.

Las manifestaciones del activismo del tercer sector (trabajando en defensa de derechos digitales) usualmente se cristalizan en manifiestos, pronunciamientos, peticiones en línea y boletines de prensa que buscan la apertura de una ventana política. Sin embargo, las siguientes actividades son impedidas:

- Trabajo a tiempo completo en la defensa de DDHH en Internet.
- Establecimiento de una agenda propositiva y no reactiva.
- Realización de estudios específicos a nivel nacional (similares a los que se realizan en otros países de la región).
- Financiamiento directo. En el período de estudio, el financiamiento de organizaciones de sociedad civil se lo realizó principalmente mediante asociación con otras instituciones previamente establecidas.
- Litigación.

Bloqueo de IPs por parte de los proveedores de Internet

En abril de 2016, el portal de denuncias anónimas Ecuador Transparente hizo público un memorando técnico de Telefónica donde referían que la Asociación Ecuatoriana de Proveedores de Internet (AEPROVI), que controla el 95% del tráfico de internet en Ecuador, "bloqueó el acceso a ciertas páginas de internet por solicitud del gobierno nacional" (Ecuador Transparente, 2016). En su boletín de prensa, Ecuador Transparente mencionaba que este memorando era consistente con documentación pública pre-existente. La Superintendencia de Telecomunicaciones (2015) señala, por ejemplo, haber efectuado "el bloqueo de dominios específicos de Internet" para combatir la piratería (p. 64). Asimismo, el reporte que presentó su centro de respuestas a incidentes informáticos, EcuCERT, a la Unión Internacional de Telecomunicaciones, reconoció que se han bloqueado e inhabilitado "dominios web (...) en cooperación con la Corporación Nacional de Telecomunicaciones y proveedores de internet privados" (Rivadeneira, 2015, p. 27).

De acuerdo a información provista por Ecuador Transparente, fueron actores de sociedad civil quienes, en conjunto con su personal, realizaron la indagación referente a la documentación, así como la coordinación con ciertos portales noticiosos en el exterior. La noticia recibió cobertura de medios de comunicación digitales y de organizaciones de sociedad civil de siete países, incluido Ecuador. Los artículos de prensa relacionados fueron referidos en redes sociales por varios periodistas de medios de prensa escrita e incluso por el expresidente de Colombia Álvaro Uribe [@AlvaroUribeVel]. Los medios digitales reportaron que las visitas el día de la publicación se contaron por miles.

A pesar de la enorme cantidad de reclamos que estas publicaciones ocasionaron, no hubo un solo medio de prensa escrita en Ecuador que cubriera el tema, disminuyendo así el alcance que pudieron llegar a tener las peticiones de organizaciones de sociedad civil, tanto para los proveedores de internet, como para el organismo regulador. Tanto Telefónica, como el gobierno nacional, han guardado silencio sobre la denuncia, a pesar de haber reconocido la misma. La Asociación de Proveedores de Internet emitió un comunicado señalando que se trataba de "información errónea" y sugirió posibles problemas técnicos como explicación a la interrupción del servicio. Según Ecuador Transparente, AEPROVI se negó a brindar datos sobre el tráfico de internet en la fecha señalada (P. Noel, entrevista, 31 de mayo de 2016).

2. Conclusión

Los actores de sociedad civil, debido a la falta de recursos financieros y administrativos producto de la actual legislación, no pueden trabajar a tiempo completo en la defensa de los derechos humanos de los usuarios de internet. Por ello, limitan sus actividades a trabajos de análisis, sensibilización y campañas públicas para la adopción de mejores prácticas, principalmente por parte del gobierno. Sin embargo, la posición antagónica que este mantiene con la prensa y las organizaciones no gubernamentales impide el desarrollo adecuado de las actividades típicamente relacionadas con la sociedad civil: transparencia gubernamental, provisión de servicios y activismo efectivo reflejado en cambios supralegales, legales e infralegales. Sin el reconocimiento del tercer sector como un actor legítimo en el escenario político por parte del gobierno, es improbable que se produzcan los cambios legales necesarios para su adecuado funcionamiento.

Bibliografía:

Ortiz Lemos, A. (2014). Sociedad civil y Revolución Ciudadana en Ecuador. Revista mexicana de sociología, 76(4), 583-612.

Delgado, J. A. (2014). Gobernanza de Internet en Ecuador: Infraestructura y acceso. Artículo presentado en el Encuentro Nacional de Gobernanza de Internet, Quito, Ecuador.

Pérez, G. (2016). Hacking Team: malware para la vigilancia en América Latina. Derechos Digitales.

Leiva, I. (2015). Hacking Team, Chile y Ecuador. Obtenido de https://people.torproject.org/~ilv/ht_chile_ecuador.html

Ministerio de Telecomunicaciones y de la Sociedad de la Información (2015, Ago. 7) Acuerdo Ministerial No. 034-2015. Registro Oficial 561.

Unit, E. I. (2015). The Economist Intelligence Unit's index of democracy 2015. The Economist.

Levi-Faur, D., & Oxford Handbooks Online Political Science. (2012). Oxford handbook of governance. Oxford: Oxford University Press.

Ecuador Transparente (2016, Abr. 14). El gobierno ecuatoriano y la Asociación de Proveedores de Internet trabajan juntos para bloquear el acceso a páginas web. Obtenido de https://ecuadortransparente.org/publicaciones/

Superintendencia de Telecomunicaciones. (2015). Informe rendición de cuentas 2014. p. 64. Obtenido de http://bit.ly/22ufifv

Rivadeneira, M. (2015). CSIRT- Supertel.

Derechos en Internet en Ecuador: más allá del acceso

Alfredo Velazco
Director de la Asociación de Usuarios Digitales de Ecuador

Ecuador, con más de 16,5 millones de habitantes hasta Abril de 2016, es uno de los países latinoamericanos que más ha implementado infraestructura de telecomunicaciones en los últimos años. Actualmente, cuenta con cerca de 60,000 km de fibra óptica que conectan casi todos los cantones del país. Pero ¿cómo toda esta infraestructura se traduce en acceso y por qué no es suficiente para ejercer libremente nuestros derechos en internet?

Sobre cuántas personas acceden a internet tenemos cifras dispares. Por un lado, se encuentran los organismos del Estado, dentro de ellos, por ejemplo, la Asamblea Nacional, en 2014, sostenía que el 50% de la población tenían acceso a internet; También, la Agencia de Regulación de Telecomunicaciones, a inicios de 2016, aseguraba que el 90% de la población tenía acceso a internet. Por otro lado, se hacen presentes organismos como el INEC que nos dice que el 50% de la población mayor a 5 años, en 2015 (metodología vía encuesta), disponía de acceso a internet, entre

algunos otros datos encontrados. Estas cifras dispares nos llevan a la conclusión de que no existe una metodología coherente en el país para medir el acceso real a internet. Tomando como punto de referencia la cifra indicada por el INEC valdría preguntarse si en la encuesta las personas contestaban sabiendo que tener planes con acceso "ilimitado" a Facebook, WhatsApp u otras aplicaciones, no es tener acceso a internet, que si conocían que la velocidad recibida generalmente no es la que les ofertan y que si sabían que el precio que pagan por el acceso a internet es uno de los más caros de la región.

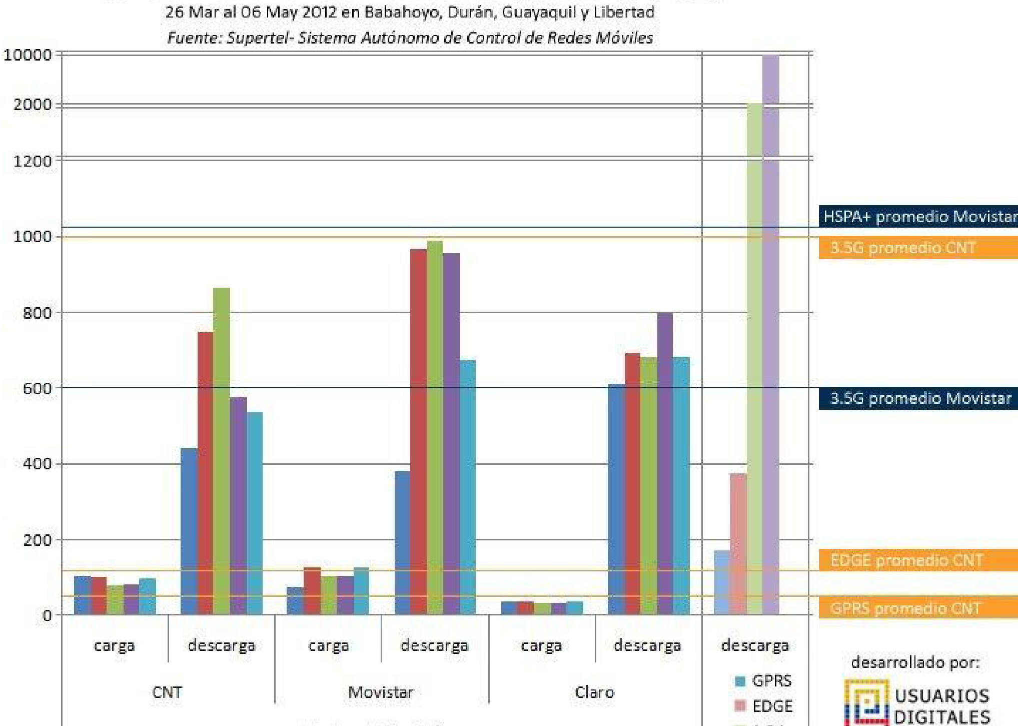
Estos datos son medulares si queremos ejercer nuestros derechos en internet. Libertad de Expresión, Privacidad, Derecho al buen nombre, Libertad de Asociación, entre otros, son derechos humanos que los podemos ejercer de manera libre en la red y deben ser protegidos, tanto online como offline, según afirma una declaración del Consejo de Derechos de las Naciones Unidas en 2012 y en una variedad de manifiestos de distintas organizaciones a nivel mundial.

1. Lo ancho de nuestra banda

Ha pasado mucha agua bajo el puente desde aquellos pitidos clásicos del modem que nos indicaban que ya estábamos conectados a la red de redes; ahora nos conectamos en silencio, de manera inalámbrica, pero lastimosamente con la misma expectativa no cumplida entre el ofrecimiento comercial y la velocidad real a la cual nos conectamos.

En Ecuador, la resolución TEL-431-13-CONATEL de 2014, de la ex CONATEL (ahora ARCOTEL), indica que la velocidad mínima efectiva de bajada de internet banda ancha es de 1024 KBPS, es decir, que banda ancha residencial (compartición 8 a 1) debería ofrecer al menos 8 MB de bajada, oferta que ni de forma comercial se realiza en el país.

La aplicación de la definición de velocidad banda ancha (fija y móvil) se cumple de manera parcial. Una muestra que realizó la agencia de control, demostró que la velocidad comercial (la de las "letras pequeñas") y la que realmente obtiene el usuario son muy diferentes:



Servicio Móvil Avanzado: Velocidad carga/descarga (kbps.) - 26 Mar al 06 May 2012 en Babahoyo, Durán, Guayaquil y Libertad - Fuente: Supertel.

Si ubicamos al Ecuador dentro del l contexto mundial, según el reporte The State of LTE de OpenSignal (Septiembre 2015), encontramos que la velocidad de bajada en tecnología LTE (pre 4G) es una de las más lentas de entre los 200 países en los que se realizó la medición.

2. El costo del acceso a internet

Aunque el gobierno ha impulsado la implementación de Telecentros (cibercafés administrados por la comunidad), el acceso prioritario se da por contratación y con un creciente impulso en cuanto a internet móvil.

Según el Reporte Análisis de precios, velocidades y asequibilidad de la banda ancha en América Latina (Enero 2016), Ecuador, en comparación con la mayoría de países de Latinoamérica, no queda en buena posición. El reporte realiza una comparación de 20 países de la región basándose en los precios relacionados al PIB per cápita; en este análisis, el plan ecuatoriano más barato de banda ancha fija está por encima del promedio de la región y el plan más barato de banda ancha móvil de Ecuador es el más caro de los países analizados.

Otro punto importante es la asequibilidad de los dispositivos, sin los cuales no es posible aprovechar el internet. Los impuestos, las salvaguardias y restricciones en cuanto a dispositivos tecnológicos han dado como resultado un aumento desproporcionado del precio al público. Esto se evidencia en una noticia de Diario El Comercio (Junio, 2015) donde se compara el precio de un celular iPhone, que en el país supera el precio al público de una gran cantidad de países con mayor nivel adquisitivo.

Este contexto impide una masificación rápida del acceso a internet y la mantiene en grupos con mayor poder adquisitivo.

3. Redes sociales ilimitadas (limitadas en sus funciones) e internet

¿Realmente los ecuatorianos nos conectamos a internet? ¿Conectarnos a ciertas aplicaciones es acceso a internet? ¿Qué nos ofrecen como redes sociales ilimitadas? Son algunas de las preguntas que la mayoría de los usuarios no las tenemos claras y que tienden a confundirnos y a crear una falsa ilusión.

Algunas estrategias han nacido de proveedores de servicios y estas han afectado el acceso real a la red, pero han sido comunicadas y asimiladas por algunos gobiernos como una solución de masificación que le ha permitido rankear al país con una mejor conectividad y, por tanto, han sido percibidas como políticas públicas. Estrategias como zero rating (aplicaciones de acceso sin cargo) o free basics (planes de acceso a determinados contenidos), que priorizan vía acceso gratuito servicios/contenidos frente a otros, crean la ilusión de acceso a la red.

En Ecuador, pese a la incidencia de la sociedad civil, por varios años, para que en la Ley de Telecomunicaciones se protege la neutralidad de la red, no se logró que estrategias como el Zero Rating dejen de ser comercializadas y se conviertan actualmente en un estándar. Y esas estrategias van aún más allá, servicios como WhatsApp, ofrecidos comercialmente como ilimitados, no se brindan de manera íntegra, ya que solo permite ciertas funcionalidades de la aplicación.

A nivel mundial, las prácticas para acceder a determinados contenidos/servicios de internet como impulso para masificarlo datan de la década de los años 90. En la actualidad, Facebook ha sido el más observado por sus iniciativas. Internet.org (presentado inicialmente como acceso gratis a internet y luego llamado free basics) es el proyecto de la red social que ha sido criticado y legalmente impedido de entrar a algunos países y afectar la neutralidad de la red. Wikipedia Zero, proyecto de la enciclopedia del conocimiento colectivo en la red, impulsa el zero rating de manera más silenciosa y eficiente, logrando entrar con su servicio de contenido gratuito a algunos países, incluso en Ecuador, a través de Movistar.

Finalmente, el tema de la neutralidad de servicios y contenido se vuelve más complejo cuando hablamos de indexarlos, es decir, que sean fácilmente encontrados en un buscador. Por ejemplo, Google, el jugador dominante en las búsquedas de la red, solo indexa una pequeña parte de toda la red, el resto es denominado deep web. ¿Acaso esta valoración de indexar o no servicios/contenidos para que sean fácilmente localizables afecta la neutralidad? Es una pregunta aún en discusión.

Bibliografía:

Consejo de Derechos Humanos de las Naciones Unidas - 20º período de sesiones - Tema 3 de la agenda: Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo https://www.facebook.com/UsuariosDigitales/photos/a.10150317193823152.338904.96481988151/10151192684598152/?type=3&theater.

Resolución TEL-431-13-CONATEL 2014 - Revisión y establecimiento de una definición para el término Banda Ancha https://www.facebook.com/UsuariosDigitales/photos/a.10150317193823152.338904.96481988151/10152279270038152/?type=3&theater.

Servicio Móvil Avanzado: Velocidad carga/descarga (kbps.) - 26 Mar al 06 May 2012 en Babahoyo, Durán, Guayaquil y Libertad - Fuente: Supertel https://www.facebook.com/UsuariosDigitales/photos/a.10150317193823152.338904.96481988151/10150952967418152/?type=3&theater.

Reporte: The State of LTE (September 2015) por OpenSignal https://www.facebook.com/usuariosdigitales/posts/10153312865663152.

Reporte Análisis de precios, velocidades y asequibilidad de la banda ancha en América latina – Enero 2016 https://www.facebook.com/UsuariosDigitales/photos/a.10150317193823152.338904.96481988151/10153574094053152/?type=3&theater.

Precio de iPhone en el país, entre los más caros del mundo (Junio 2015) https://www.facebook.com/UsuariosDigitales/photos/a.10150317193823152.338904.96481988151/10153062369038152/?type=3&theater.

Ley de Telecomunicaciones y Neutralidad de la Red – caso Whatsapp https://www.facebook.com/notes/usuarios-digitales/ley-de-telecomunicaciones-permite-restringir-llamadas-por-whatsapp/10152900078508152.

Internet.org – Free Basics de Facebook
https://info.internet.org/es/.

Wikipedia Zero - detalles
https://es.wikipedia.org/wiki/Wikipedia_Zero.

Deep Web
https://es.wikipedia.org/wiki/Internet_profunda.

Entender, usar, crear y desafiar el Internet

Daniela Viteri
Observatorio de la Juventud para América Latina y el Caribe

En un mundo globalizado e hiperconectado, el Internet es un elemento clave para la competitividad en especial entre las nuevas generaciones. Las tecnologías de información y la comunicación (en adelante TIC) son elementos necesarios para poder alcanzar un desarrollo con más equidad, mayor crecimiento e innovación. Internet, hoy en día, llega a ser utilizado por casi cuatro mil millones de personas en el mundo. ¿Nos hemos preguntado quienes son las personas que más lo utilizan? Varias estadísticas de la ONU demuestran que la mayoría de usuarios son jóvenes entre los 18 y 30 años. Inclusive, el organismo especializado de las Naciones Unidas para las Tecnologías de la Información y la Comunicación (UIT) explica que el 30% de estas personas son "nativos digitales"[1] . El "concepto de nativo digital alude a los usuarios posteriores a los medios interactivos como Internet y las pantallas; además hace una diferencia conceptual entre el antes y el ahora, entre sociedad de la información y sociedad del conocimiento" (Ibarra y de la Llata, 2010). Identificar los mayores consumidores de Internet permite entender por un lado el

1 Comunicado de Prensa de la UIT desde Ginebra, el 7 de octubre de 2013.

crecimiento de la industria (con el objetivo de proporcionar dispositivos, servicios y plataformas que respondan a sus necesidades específicas en el mercado de la tecnología) y por otro los comportamientos de los usuarios (para ofrecer plataformas de información, educación, interacción, entretenimiento, etc.). En este sentido, se ha identificado que Latinoamérica tiene la mayor proporción de usuarios de Internet menores de 25 años en todo el mundo[2]. Según el Informe de Desarrollo Mundial de 2015 del Banco Mundial[3], los jóvenes son los principales consumidores de contenidos digitales ya que utilizan más de 27 minutos en línea por cada conexión establecida. Además estos representan el 42,4% de la población mundial y son el 45% de los usuarios de Internet (UIT, 2015). Delimitar quiénes conforman la mayor cantidad de los usuarios es fundamental pues permite a los actores detrás de la industria, en especial quienes definen la creación de políticas y regulación, comprender cómo es que los jóvenes entienden, usan, crean y desafían el Internet.

Quienes trabajan para la industria de Internet deben invertir esfuerzos para determinar las prácticas de consumo y las formas de sociabilidad de los jóvenes en Internet. Por esta razón grandes empresas están destinando millones de dólares a la investigación del comportamiento de estos usuarios y el impacto del internet en sus vidas. Por ejemplo, CISCO[4] entrevistó a grupos de estudiantes universitarios y a jóvenes profesionales a nivel mundial para poder entender qué significa el internet para ellos. Los datos de la investigación revelaron varios aspectos importantes de la vida cotidiana que evidencian la alarmante dependencia a internet: 2 de cada 3 entrevistados escogieron internet por sobre un automóvil y 1 de cada 3 argumentaron que es igual de importante que el agua, el alimento y el aire. El 55% de la muestra poblacional de este estudio respondieron que no podría vivir sin internet. La investigación demostró la necesidad de poseer este servicio a través de una pregunta que rankea si el internet es más importante que tener citas, salir con amigos, ir a una fiesta o escuchar música; la respuesta fue "sí" para 2 de cada 5 personas. Las redes sociales[5] son parte de la vida de los jóvenes y de los usuarios, puesto que 1 de cada 4 entrevistados explicaron que mantenerse actualizados en Facebook es importante. Más del 65% posee un dispositivo móvil y considera a la tecnología como lo más importante en su vida. Las preferencias entre ordenadores y móviles se reduce cada día más y las aplicaciones han remplazado herramientas de la vida cotidiana (por ejemplo, los periódicos, las agendas, etc.). Estos datos demuestran la necesidad de plantear nuevas estrategias de consumo de internet para el futu-

---

2 Estrategia del PNUD para la Juventud del 2014 al 2017.

3 Varios informes del Banco Mundial que datan del 2015 demuestran la desigualdad de acceso a la revolución digital.

4 CISCO. El mundo conectado de Cisco: Seguridad móvil internacional: Datos claves y consideraciones extraídos del estudio para la TI de la empresa.

5 Entendidas como herramientas de comunicación muy potentes, permiten ver e insertar fotografías, vídeos y enviar mensajes entre usuario, según el Instituto de Tecnologías Educativas del Ministerio de Educación del Gobierno de España.

ro, en tanto que el patrón de comportamiento histórico refleja un aumento en el uso del servicio de internet. En este marco, factores como acceso, infraestructura y costo deben tomarse en cuenta, en el caso de los jóvenes incluso determinando los dispositivos y lugares en los que utilizan el servicio. En conclusión, los patrones de comportamiento de la comunidad internauta tendrían que delimitar la regulación de internet y la toma de decisiones cuando se diseñen las respectivas políticas públicas, de manera que estas se acerquen y respondan a las necesidades y expectativas de la mayoría de usuarios. Para lograr diseñar un buen marco de regulaciones y políticas públicas que se acerque a los internautas, hay que regresar a comprender cómo empezó a controlarse el Internet.

Desde sus inicios, el internet ha evolucionado de manera vertiginosa, en cuanto a condiciones jurídicas, políticas, económicas y sociales, desde una dinámica pionera en la socialización de actores y los acuerdos multisectoriales. La Organización de Naciones Unidas hace 10 años decidió crear un espacio internacional de diálogo sobre el desarrollo del mismo, tomando en cuenta el alto impacto que este tenía en el comportamiento de la sociedad, y el potencial que preveían. En julio de 2006[6], el Secretario General de las Naciones Unidas anunció oficialmente el establecimiento de un Foro de Gobernanza de Internet (en adelante IGF por sus siglas en inglés) que buscaba incluir a todos los actores alrededor de la gobernanza. Esto permitió la creación de un espacio de diálogo inclusivo, en el que sectores como gobiernos, empresas, sociedad civil, comunidad técnica y la academia puedan exponer sus posturas en igualdad de condiciones bajo procesos abiertos. Para el año 2015, el IGF tenía una agenda que debía abordar varios temas inmediatos, entre ellos demostrar los frutos de 10 años de gestión, puesto que en la Asamblea General del 2016 se debía renovar el mandato del foro luego de una rendición de cuentas. De aquí partió la necesidad de reinventar este espacio, recuperando las bases en las que se había constituido. Es decir que sea innovador e inclusivo para un mejor empoderamiento de las buenas prácticas que habían realizado los últimos 10 años alrededor del internet y las nuevas tecnologías. Tomando en cuenta la necesidad de un internet inclusivo, innovador y realista, se logró reconocer la importancia y necesidad de oír el interés de los jóvenes, sus ideas, motivaciones y proyectos.

Internet Society, como la principal fuente independiente mundial de confianza sobre políticas, estándares tecnológicos y desarrollo del futuro de internet, define a la Gobernanza de Internet como:

> …los procesos y normas que afectan la forma en que se gestiona Internet. El éxito histórico y futuro de Internet como plataforma abierta y confiable para la innovación y el empoderamiento depende de la adopción de un enfoque descentralizado, colaborativo y de múltiples partes interesadas hacia la Gobernanza de Internet.

6 Foro de Gobernanza de Internet.

Esto permite a varios actores participar en los procesos que hacen que internet siga creciendo y evolucionando como una plataforma de innovación, desarrollo económico y progreso social para las personas de todo el mundo. En los últimos meses, se ha logrado analizar el rol de la juventud en la Gobernanza de Internet. Esto se debe a que los jóvenes a nivel mundial enfrentan varios retos en cuanto a acceso, conectividad y educación, a pesar de ser los mayores consumidores. Las problemáticas detalladas a continuación no excluyen otros inconvenientes, sin embargo, se detallarán aquellas que han sido identificadas para poder ampliar el diálogo con el fin de solucionar dichos problemas.

La Gobernanza de Internet es un espacio de diálogo abierto, dedicado a gestionar y a abordar problemas desde distintas perspectivas. Los jóvenes, en la actualidad, tienen varios espacios para participar de este diálogo, existen iniciativas desde ICANN, ISOC (Internet Society), empresas como Google, Facebook, Twitter y varias organizaciones de la sociedad civil que organizan encuentros, foros y distintos proyectos para involucrarlos. En 2015, el Comité Gestor del Internet de Brasil junto a Internet Society, lanzaron el programa *Youth IGF*. Este programa buscaba introducir a jóvenes de la región en temas relacionados con la Gobernanza de Internet. A través de cursos en línea, 150 jóvenes fueron capacitados sobre Gobernanza de Internet, ecosistema de la red, infraestructura, estándares, protocolos y principios de internet. De allí, se escogieron 50 jóvenes que continuaron con actividades preparatorias para la última edición del Foro de Gobernanza de Internet. Por iniciativa de este grupo de jóvenes, se formó el primer Observatorio de la Juventud para América Latina y el Caribe. Este observatorio buscaba solucionar las problemáticas antes mencionadas.

Si bien la participación activa de jóvenes en el ecosistema es muy distante aún, para febrero de 2016 se logró consolidar el primer Observatorio a nivel de Latinoamérica y el Caribe conocido como Youth Observatory. El principal objetivo es crear una plataforma que provea de la mayor cantidad de recursos y oportunidades para la integración de jóvenes en el mundo de la Gobernanza de Internet. Por esta razón las plataformas utilizadas son abiertas, como Facebook o Telegram, para garantizar una red con mayor alcance, en los idiomas más utilizados en el continente (español, inglés y portugués). También se hablaría del desafío de obtención de recursos económicos, no solo inmediatos, sino sostenibles en el tiempo. Y, por último, se puede hablar sobre la brecha estructural que enfrentan los jóvenes en la Gobernanza de Internet con respecto de las políticas públicas, tanto a nivel internacional como local. En conclusión es valioso reconocer las iniciativas que se han creado alrededor de la región con una visión inclusiva, diversa y dinámica que responda a las necesidades de los jóvenes perpetrando su participación.

Por un lado podemos tomar en cuenta que los jóvenes son los consumidores más importantes, y teniendo como premisa que el internet es parte de sus vidas, se entiende que usen las estructuras existentes para que sus necesidades sean las

que moldeen el curso del internet. En este marco, asumimos que las empresas, gobiernos y otros actores requieren saber las necesidades, el comportamiento y el lenguaje que se utiliza actualmente para poder utilizar el internet de manera rentable, funcional y eficaz. En este sentido, aún hay pocos involucrados en el tema de la Gobernanza de Internet y hay mucho trabajo que hacer en términos de pedagogía y comunicación. Tomando en cuenta que hay un alto porcentaje de personas que aún no tienen acceso a internet, no sorprende que en muchas comunidades, incluso en varios países, el término de "Gobernanza de Internet" sea algo nuevo que no ha sido abordado ni transmitido. Es importante reconocer que el gobierno no puede ser el único actor que dé estos espacios, puesto que mucho del "*Know-how*" y de la creatividad se desarrolla desde las empresas y en la sociedad civil (Baird, 2009), y, de manera vertiginosa, son los jóvenes quienes van creando más información, contenido, software y aplicaciones en el internet. Es por esta razón que las iniciativas de involucrar a jóvenes requieren de mucha difusión y apoyo económico para hacerse conocer. El Observatorio ha creado varias estrategias de difusión de información inclusivas y ha utilizado las, redes sociales para aumentar la conciencia del diálogo y la participación activa. Por consiguiente, el reto para conseguir mayor participación de los jóvenes es encontrar las mejores estrategias para llegar a esta población demográfica y explicar la importancia del tema.

Por otro lado es necesario analizar el problema del sustento económico, que responde a encontrar financiación a largo plazo, ya que es un reto difícil de superar. Es importante reconocer que los jóvenes usualmente no tienen ingresos, por lo que costear su participación en foros nacionales, regionales o internacionales de Gobernanza de Internet podría no ser una opción o prioridad. Sin embargo, visibilizar la participación y ejecución de las innovaciones y proyectos es fundamental. Por consiguiente se requiere un recurso económico que solvente pasajes, hospedajes y otros costos como incentivo para la participación. La mayoría de reuniones solucionan este inconveniente con una bolsa de becas abiertas al público. A través del Observatorio de la Juventud, al ser un capítulo de interés perteneciente a Internet Society, se ha creado una bolsa de becas específicamente para personas de 18 a 30 años. Esta es una solución temporal, puesto que buscamos que más jóvenes se integren en el diálogo y su participación sea mayor, por lo que pronto este único recurso de financiación será escaso. De allí parte la necesidad de encontrar jóvenes que apoyen con iniciativas, proyectos y soluciones rentables, funcionales y sostenibles en el futuro, iniciativas que sean inclusivas y diversas y que respeten la naturaleza *multistakeholder* del internet.

Por último, un problema que debe superarse es la brecha que existe desde una perspectiva de edades en la discusión de políticas alrededor de la Gobernanza de Internet, dado que actualmente hay pocos jóvenes tomados en cuenta. Se ha mencionado la creación de un Observatorio a nivel regional, pero aún hay pocos canales y espacios que integren las voces de los jóvenes. Este inconveniente se replica en los gobiernos comunitarios, nacionales, regionales e internacionales. Que los jó-

venes se involucren ha dejado de ser una discusión y ha pasado a ser una necesidad en los diferentes sectores de la Gobernanza de Internet. Vint Cerf, en su calidad de Vicepresidente Mundial de Google y padre del internet, ha denunciado que "si no se toman en cuenta las ideas de los jóvenes en consideración, todos los principios de gobernanza que se adopten van a fallar", puesto que los tomadores de decisiones pertenecen a otra generación que no logran abstraer que hacen o que saben los jóvenes actualmente, entonces "las reglas y normas que se inventen o desarrollen no serán relevantes" para ellos, que son los mayores consumidores y usuarios. Esto demuestra la necesidad de desarrollar el internet alrededor de los consumidores actuales, que son quienes pueden transmitir las necesidades, innovar y satisfacer sus ambiciones. Esto, a su vez, permite reducir la brecha estructural que existe a través de la participación activa. Por consiguiente, los jóvenes se ven involucrados no solo en las temáticas de Gobernanza del Internet, sino también en la implementación de políticas públicas que aborden los inconvenientes de sostenibilidad.

En conclusión, es una necesidad involucrar a los jóvenes en todos los ámbitos alrededor de la Gobernanza de Internet, para que la toma de decisiones sea una respuesta a las expectativas y requerimientos de los actuales y futuros usuarios. Es fundamental aumentar su participación en los espacios de diálogo y en el desarrollo de políticas públicas, en tanto que los jóvenes son los mayores consumidores de internet en la actualidad y el crecimiento es exponencial. En el caso del Ecuador, el uso de internet también está en constante cambio. De acuerdo a las últimas estadísticas del Observatorio TIC del Ecuador y el Ministerio de Telecomunicaciones y de la Sociedad de la Información, desde el año 2010 hasta el año 2014 ha habido un aumento del 20.6% en cuanto a uso de internet. Enfatizan que el 4.3% de los ecuatorianos utiliza el internet mensualmente, 35.5% semanalmente y a diario el 60.2%. En el Ecuador, el 13% de la población está representada por jóvenes (personas de 18 a 24 años)[7]. Los datos del Instituto Nacional de Estadísticas y Censos (INEC), en cuanto a jóvenes y tecnología han encontrado que el 52,5% ha utilizado una computadora en el último año. El 46,5% ha logrado acceder a internet en el mismo período de tiempo y un 57,5% de los jóvenes posee un celular. Estas cifras son un referente de los consumidores de internet a nivel nacional, que con el tiempo ha aumentado no solo en cantidad, sino también en calidad. El panorama es similar en la región y el debate para abordar las necesidades de los consumidores cada vez es más inclusivo con los diferentes usuarios. En el Ecuador, los jóvenes tienen poca participación activa en este tema, por no decir nula. Sin embargo, hay esfuerzos de colectivos y la sociedad civil que han creado pocos espacios para escuchar sus ideas, proyectos y perspectivas.

La difusión, educación y capacitación de la Gobernanza de Internet en el país es algo que se debe empezar a transmitir a fin de reducir brechas de acceso y generar nuevas oportunidades. El internet es una herramienta que pasó de ser un lujo a un

7 INEC (Instituto Nacional de Estadística y Censo). Ecuador.

servicio necesario, puesto que es un instrumento que brinda acceso a educación, información y conectividad. Al ser la red de redes que se va tejiendo cada minuto, debemos entender la importancia de participar activamente como jóvenes y generar los espacios que permitan explotar las capacidades y destrezas, de sumarnos al diálogo sobre la gobernanza y gestionar el cambio. Abrir las puertas a la juventud, en calidad de actor en la Gobernanza de Internet, permitiría que a medida que vaya creciendo el tema y la concientización, se lo haga con jóvenes educados y capacitados en el respeto a los principios básicos de un internet libre y democrático. Por esta razón es importante reconocer que el patrón de comportamiento de los jóvenes busca entender, usar, crear y desafiar el internet para solventar una problemática social, política y económica en nuestra sociedad.

Bibliografía:

Banco Mundial. (2015). Informe sobre el desarrollo mundial 2015. Tomado desde http://hdr.undp.org/sites/default/files/hdr_2015_report_sp.pdf.

Banco Mundial. (2015). Informe Anual 2015. Tomado desde http://www.bancomundial.org/es/about/annual-report.

Baird, Z. (2002). Governing the Internet: Engaging government, business, and nonprofits. Foreign Affairs, 81(6), 15-20. Tomado desde https://www.foreignaffairs.com/articles/2002-11-01/governing-internet-engaging-government-business-and-nonprofits.

CISCO. (2013). El mundo conectado de Cisco: Seguridad móvil internacional: Datos claves y consideraciones extraídos del estudio para la TI de la empresa. Tomado desde http://www.cisco.com/c/dam/global/es_es/assets/pdf/byod_connected-world_cte_report_es.pdf.

Foro de Gobernanza de Internet. Tomado desde http://www.intgovforum.org/cms/aboutigf.

Ibarra, A. M., y de la Llata, D. E. (2010). Niños nativos digitales en la sociedad del conocimiento; acercamientos conceptuales a sus competencias. Razón y palabra, ISSN-e 1605-4806, Nº. 72, 2010, 24 págs. Tomado desde http://www.razonypalabra.org.mx/N/N72/Varia_72/14_Ibarra_72.pdf.

Instituto Nacional de Estadística y Censos. http://www.inec.gob.ec/inec/index.php?option=com_content&view=article&id=23%3Alos-jovenes-representan-el-13-de-la-poblacion-ecuatoriana-dia-internacional-de-la-juventud-&catid=63%3Anoticias-general&lang=es.

Instituto de Tecnologías Educativas del Ministerio de Educación del Gobierno de España. Adolescentes y redes sociales. Tomado desde http://www.ite.educacion.es/formacion/materiales/157/cd/m6_1_redes_sociales/adolescentes_y_redes_sociales.html.

Observatorio de la Juventud para América Latina y el Caribe. Tomado desde http://obdjuv.org/.

Pérez, J. y Olmos, A. (2009). Introducción: Gobernanza de Internet. Tomado desde https://telos.fundaciontelefonica.com/telos/articulocuaderno.asp@idarticulo=1&rev=80.htm.

Programa de Naciones Unidas para el Desarrollo. (2014), Estrategia del PNUD para la Juventud 2014-2017. Tomado desde http://www.undp.org/content/dam/undp/library/Democratic%20Governance/Youth/UNDP-Youth-Strategy-2014-2017-SP.pdf.

Protección Online. (2013). Infografía: Los jóvenes y el uso de internet. Tomado desde http://www.protecciononline.com/infografia-los-jovenes-y-el-uso-de-internet/.

UIT (Unión Internacional de Telecomunicaciones). 2015. ICT Facts and Figures: The World in 2015. Tomado desde www.itu.int/ en/ITU-D/Statistics/Pages/stat/.

UIT (Unión Internacional de Telecomunicaciones). 2015. Cominicado de Prensa. Ginebra, octubre del 2013. Tomado desde http://www.itu.int/net/pressoffice/press_releases/2013/41-es.aspx#.WAMhuuDhCM8.

Winocur, R. Internet en la vida cotidiana de los jóvenes. Revista Mexicana de Sociología del Instituto de Investigaciones Sociales de la Universidad Nacional Autónoma de México Universidad Nacional Autónoma de México. Vol. 68, No. 3 (Jul. - Sep., 2006), pp. 551-580. Tomado desde http://www.jstor.org/stable/20454250.

Working Group of Internet Governance (WGIG) (2005, junio). Report of the Working Group on Internet Governance [en línea]. Disponible en: http://www.wgig.org/docs/WGIGREPORT.pdf.

TERCERA PARTE
OBSERVACIONES AL PROYECTO DE LEY ORGÁNICA DE PROTECCIÓN DE LOS DERECHOS A LA INTIMIDAD Y PRIVACIDAD SOBRE LOS DATOS PERSONALES

Observaciones al Proyecto de Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales

El 12 de julio de 2016, se presentó en la Asamblea Nacional el proyecto de Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales. El 8 de septiembre, el Colegio de Jurisprudencia de la Universidad San Francisco de Quito, con el apoyo de Google Inc., realizó el Seminario "Desafíos de la reglamentación sobre protección de datos para Ecuador y la promoción del comercio electrónico y los negocios sobre Internet". Este evento académico centró su análisis en el referido Proyecto de Ley Orgánica. El presente documento sistematiza las observaciones generales y específicas que se plantearon al proyecto de ley. El documento se divide en seis secciones: a) para qué la ley b) aspectos formales de técnica legislativa; c) comentarios generales; d) observaciones de fondo, e) comentarios específicos al articulado; y f) conclusiones.

1. El para qué de la ley

1. En términos generales, la ley debe garantizar la protección de los derechos a la intimidad y privacidad; el derecho a expresarse y ser informado; así como el fomento y desarrollo de la innovación tecnológico.

2. El proyecto contiene dos páginas de considerandos, en las que se enumeran cuerpos legales que ya regulan temas relacionados con el registro y protección de datos públicos.

3. Ante esto, cabe preguntarse si en realidad se requiere una ley específica dedicada al tema o, únicamente, introducir en la legislación vigente (pensemos, por ejemplo, en la Ley del Sistema Nacional de Registro de Datos Públicos) aquellos temas que se considere faltantes en la misma, o que sea del caso modificar.

4. Parece que lo más adecuado no es un nuevo cuerpo normativo, sino únicamente un conjunto de reformas a la legislación existente. De esa manera se mantiene coherencia con la política de codificación normativa, que se ha puesto en práctica en el último tiempo, y se contribuye a disminuir la dispersión legislativa.

2. Algunos temas de técnica legislativa

1. Los dos primeros artículos del proyecto son repetitivos e innecesarios. Por otro lado, incluir en el texto el objeto y el ámbito de aplicación de la ley, cosa que se ha vuelto común en los últimos tiempos, solo tiene sentido cuando la norma rige para materias o espacios específicos y no, como en este caso, cuando se trata de reglas de aplicación general en todo el territorio nacional. Tanto el ámbito, como el objeto de la ley, se desprenden del texto de la misma, y no es necesario referirse a ello expresamente.

2. Un glosario de términos, como el que aparece en el artículo 4, se justifica cuando las palabras tienen un uso diferente del propio del lenguaje común, o cuando debe precisarse su significado. En esa medida, muchas de las definiciones que aparecen en el proyecto son innecesarias; piénsese, por ejemplo, en base de datos, consentimiento del titular, usuario de datos, etc.

3. Puesto que la organización institucional de la Función Ejecutiva corresponde al Presidente de la República, no deben mencionarse, en una ley, ministerios de estado determinados o unidades administrativas de los mismos. En el artículo 11, por eso, debería hablarse en general de la Función Ejecutiva o del Ministerio del ramo, y no de un Ministerio en concreto.

4. El artículo 18 recoge una norma uruguaya sobre inscripción de bases de datos, norma que es preciso corregir a fin de adecuarla a la terminología jurídica ecuatoriana; en el número 6, en lugar de personas físicas, debe hablarse de personas naturales.

5. Se recomienda eliminar del proyecto todas las alusiones a términos que no son de uso en nuestra realidad y ordenamiento jurídico y que evidencian que el proyecto incluye normativa propia de otras latitudes. Por ejemplo el término ficheros en los artículos: 9, 10, 14, 15, 18, 19, 26, etc.

3. Comentarios generales

1. La protección de datos es una materia con carácter transversal en la sociedad, que repercute en muchas áreas, industrias y sectores productivos; y que debe ser observada tanto por actores privados como públicos, por lo que la elaboración de una norma debe considerar su incidencia y repercusión en éstos ámbitos.

2. La Ley debería proteger el derecho a la autodeterminación de las personas y garantizar el derecho a la privacidad a través de una regulación que determine el legítimo e informado sobre el tratamiento de los datos.

3. Al ser la Ley de Protección de Datos Personales una materia jurídica que

se enmarca dentro de la rama del derecho administrativo, sus disposiciones deben ser claras y precisas sin dejar espacios abiertos o normas subjetivas o en blanco que se podrían prestar a confusión o a excesos.

4. Las infracciones y sanciones deben estar expresamente tipificadas por Ley de acuerdo a la Constitución, lo cual implica que al redactarse se debe determinar claramente su alcance y no dejar opción a interpretaciones.

5. La regulación en protección de datos personales puede ser una herramienta para promover y fomentar el progreso tecnológico, desarrollo de contenidos y aplicaciones, el comercio electrónico y el emprendimiento en general, o puede también tornarse en un instrumento que desincentive el desarrollo de la industria digital, por las restricciones, los controles, cargas o requisitos que podría exigir la normativa frente al dinamismo y rapidez que demanda el entorno digital.

6. La norma otorga al Ejecutivo (a través de la Autoridad Nacional de Protección de Datos Públicos) la facultad de ejercer vigilancia y control sobre los datos, lo mismo podría atentar contra los principios de la libertad de expresión al dejar abierta la posibilidad de un bloqueo a los sistemas informáticos, páginas web, blog o similares, en nombre de la protección de datos personales.

7. El marco normativo deja la posibilidad de tipificar el "Derecho al Olvido", la cual no es una figura jurídica delimitada. Siguiendo los casos en países como España o Chile, en donde la amenaza recae en la baja de información considerada como personal o de intimidad que resulta ser de interés público. Por ejemplo, el caso de que una figura pública quiera eliminar o des-indexar información que cuestione su integridad. Es decir, por una defensa a la protección del honor (un derecho consagrado por la Constitución), se puede utilizar de causal para la baja de columnas de opinión, noticias, entre otros.

4. Los temas de fondo

<u>Sobre la Autoridad Nacional y el registro de bases de datos</u>

1. El artículo 11 establece una Autoridad Nacional de Protección de Datos Personales, como ente de la Función Ejecutiva.

Si tomamos en cuenta que parte del trabajo de la referida Autoridad será el control de bases de datos manejadas por la propia Función Ejecutiva, resulta clara la inconveniencia de lo previsto en el proyecto, pues estaríamos afectando la necesaria independencia que debe caracterizar a todo ente controlador.

2. Se recomienda, por eso, asignar las funciones de Autoridad Nacional a un ente autónomo, existente o por crearse, pero fuera del espacio de influencia

de los entes administrativos a ser controlados.

3. Es cuestionable, por otra parte, la conveniencia del registro de bases de datos personales, que se regula en el Título IV del proyecto. No se ve la utilidad de mantener ese registro, pues el cumplimiento de las normas del resto del proyecto no depende de su existencia o inexistencia y, más bien, se estaría creando una formalidad sin mayor sentido, que contribuiría únicamente al incremento de la carga burocrática.

Sobre los poderes de la Autoridad Nacional

1. Una Autoridad Nacional como la que plantea el proyecto, debería contribuir a la protección de los derechos de las personas afectadas por la difusión de sus datos personales, y no convertirse en un ente controlador de las bases de datos, pues ello terminaría afectando otros derechos.

2. Es por eso muy preocupante la facultad que el número 3 del artículo 12 del proyecto, confiere a la referida autoridad, para bloquear temporal o definitivamente sistemas de información, por un lado porque es un poder excesivo, ya no sobre bases de datos, sino sobre la totalidad de los sistemas de información.

3. A esto se suma el hecho de que el ejercicio de la referida potestad no tiene regulación alguna, no se determinan los casos en que podrá hacérselo, no se fija un procedimiento ni aparece siquiera como una posible sanción. Es, simplemente, un poder omnímodo para decidir cuales sistemas informáticos funcionan y cuáles no.

4. Resulta cuestionable el otorgar a la Autoridad Nacional el poder, por un lado, de determinar la responsabilidad de las infracciones a la Ley y, por otro, la facultad de imponer las sanciones que podrían ser desproporcionadas y excesivas.

Sobre la indeterminación legislativa

En general, se ve a lo largo del proyecto un peligroso recurso a los conceptos indeterminados y a la falta de precisión legislativa, lo que deja en manos de la autoridad decidir a su arbitrio la mayoría de casos. Los siguientes ejemplos muestran cómo la aplicación de la ley dependerá de los entendidos de los funcionarios de turno, y no del contenido del mandato legislativo:

1. ¿Cómo deben entenderse conceptos como seguridad nacional, orden, seguridad y salud públicos, que constan en el artículo 2 y justificarán las limitaciones a principios y derechos previstos en el proyecto?

2. El artículo 3 habla de principios generales de protección de datos personales. ¿Cuáles son esos principios? ¿Quién los define?

3. ¿Cuál es el alcance de la expresión riesgo cierto de afectación de derechos, que justifica el ejercicio de una potestad absolutamente exorbitante que se confiere a la autoridad Nacional, y que consta en el número 3 del artículo 12?
4. ¿Cuál será el debido proceso que se exige en el número 8 del artículo 12, que garantice el cumplimiento de otros derechos, para determinar responsabilidades de las infracciones y sanciones que responden a los lineamientos del Título VI?
5. ¿Cuáles son los niveles de protección de datos a los que se refiere el artículo 20?
6. ¿Qué debemos entender por mal manejo del archivo y tratamiento de base de datos, que consta en el número 4 del artículo 24?

<u>Sobre el procedimiento sancionador</u>

En materia de sanciones se identifican dos deficiencias.

1. La primera tiene que ver con el hecho de que los temas procedimentales se dejan en manos de la autoridad, lo que abre la puerta a posibles arbitrariedades (artículo 28). Lo conveniente sería fijar un procedimiento en la propia ley, o remitirse a procedimientos generalmente utilizados en el Ecuador, como los que constan en el Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva o que en un futuro constarán en el Código Administrativo.
2. La infracciones se clasifican en leves (artículo 24) y graves (artículo 25), pero no ocurre lo mismo con las sanciones, que son las mismas para todos los casos (artículo 26) y que quedan libradas a una graduación que se entrega a la autoridad, otra vez revestida de un excesivo poder que se presta para actuaciones arbitrarias.

A cada infracción o grupo de infracciones, debería corresponder una sanción determinada, que podría agravarse o atenuarse a partir de criterios como los que constan en el artículo 27.

<u>Sobre el impacto económico</u>

1. De aprobarse la normativa, existen posibles desincentivos económicos como consecuencia del posible desincentivo a la inversión en las empresas. El mismo resultado se explica por la ambigüedad de la normativa, que impide tener certeza y reglas de juego claras en la industria.
2. Existe el riesgo de no encontrar un balance y equilibrio entre la protección a los derechos de intimidad y privacidad de los ciudadanos y el principio del libre flujo de información en Internet al no tener claramente delimitados los causales de un infracción a la Ley.

5. Comentarios específicos al articulado

1.- Considerandos:

En los considerandos (párrafo 9) existe un error al referirse a la normativa vigente sobre protección de datos personales, se hace referencia al artículo 78 de la Ley de Comunicación, lo correcto es el 78 de la Ley Orgánica de Telecomunicaciones.

2.- Ámbito de Aplicación

En el artículo 2 del proyecto se determina el ámbito de aplicación de la norma. En vista de que se parte de la regla general de que todos los datos personales registrados en cualquier base de datos, deben ajustarse al cumplimiento de la Ley. Es primordial definir con claridad qué tipo de información no se encuentra comprendida en el ámbito de aplicación de la norma. Las excepciones deben estar claramente identificadas, como son:

- Bases de datos creadas y mantenidas por personas naturales para el desarrollo de actividades personales o domésticas o relacionadas con su vida privada o familiar.
- Bases de datos referidas a personas jurídicas.
- Bases de datos sobre temas de seguridad nacional.
- Bases de datos para efectos periodísticos, artísticos o literarios.
- Bases de datos con información de interés público.

3.- Principios Generales

El Art. 3 del Proyecto se refiere a los principios que están obligados a observar los involucrados en la formación y manejo de bases de datos.

Legalidad: El proyecto establece que la formación de las bases de datos será lícita cuando hayan sido obtenidas por medios legítimos y se encuentren debidamente inscritas.

El principio de legalidad hace relación al cumplimiento de la normativa legal y a la licitud en la forma de obtención de la información, más no la obligación de registro. La legalidad de una base de datos no viene dada por el registro del mismo, que constituye un requisito formal, de carácter administrativo.

Adicionalmente el artículo 3.1 adolece de un error en la redacción “inscritas” y no “inscrita”.

Veracidad: En el numeral 3 al referirse a la Veracidad como principio general para el tratamiento de los datos, se señala que la recolección deberá ser veraz y no excesiva y luego se añade: "que no podrá obtenerse por medios fraudulentos, abusivos o contrarios a la Ley".

Esta última condición hace relación a la legalidad de los datos y no a la veracidad. Estas ambigüedades suponen la posibilidad de un tratamiento de datos personales como inveraz. Esto sería riesgoso, pues tiene rasgos del conocido "Derecho al Olvido" que al no estar delimitado es una categoría jurídica ambigua, que pone en riesgo el acceso a la información de interés público, y además se opone al derecho consustancial como es la Libertad de Expresión.

Reserva: Al referirse a la reserva, el proyecto dispone que las personas naturales o jurídicas que obtengan legítimamente información proveniente de una base de datos están obligadas a usarla en forma reservada y exclusivamente para las operaciones habituales de sus actividades, siendo prohibida la difusión a terceros; mientras que nuestra Constitución en el Art.92 inciso segundo dispone que ."....Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley."

En consecuencia, el proyecto de Ley establece una prohibición absoluta, no contemplada en la Constitución.

4.- Datos Sensibles

El proyecto de ley en su artículo 5 al referirse al Tratamiento de Datos Sensibles establece que está prohibido el tratamiento de datos sensibles, y determina algunas excepciones, entre ellas: el numeral 1 se refiere a que el titular autorice expresamente y por escrito el tratamiento.

La Constitución del Ecuador contempla la posibilidad del tratamiento de datos sensibles, sujetando el mismo a ciertas condiciones, así en el artículo 92 inciso tercero determina que ".... en el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias..."

En este sentido, el artículo relacionado a los Datos Sensibles establece la prohibición como regla general, mientras la Constitución reconoce la posibilidad de su archivo, siempre y cuando se cumplan ciertos requisitos. A fin de guardar armonía con el texto constitucional dicha disposición podría establecer que el tratamiento de los datos sensibles estará sujeto a determinadas exigencias, acordes al entorno digital actual.

Por otro lado, el consentimiento para el tratamiento de datos sensibles debería ser a través de un medio expreso, ya sea físico o digital. No existe ninguna justificación ni evidencia de mayor protección para que el consentimiento deba ser

ofrecido por medios escritos o físicos. Esta disposición puede afectar el comercio electrónico y va en contra de la promoción de uso de medio digitales, acción que ha sido promovida por políticas públicas conocidas como "cero papeles".

Al respecto, el Código Orgánico General de Procesos dispone que: "Artículo 202.- Documentos digitales…. Podrá admitirse como medio de prueba todo contenido digital conforme con las normas de este Código, otorgándoles igual validez que los documentos escritos; lo cual a su vez va en sintonía con el entorno digital actual.

5.- Derechos Niños, Niñas y Adolescentes

"Artículo 7.- Derechos de las niñas, niños y adolescentes (...) se prohíbe el tratamiento de sus datos personales, salvo aquellos datos que sean de naturaleza pública".

No todo tratamiento de datos personales es negativo en sí mismo. El tratamiento de datos personales de menores de dieciocho años, sujeto a ciertas condiciones, puede servir para ofrecerle un mejor acceso a contenidos e información adecuados siempre que sea realizado conforme a los principios de tratamiento de datos personales.

6.- Consentimiento

El artículo 3.4 manifiesta que el "Consentimiento Informado" deberá ser "libre, expreso, previo e informado"; sin embargo, el artículo 4.2 al referirse al "Consentimiento del Titular": omite la mención a la característica de "expreso" y hace relación a otras características como: "inequívoca, específica". Estas distintas definiciones del Consentimiento generan confusión, más aún cuando el consentimiento es un término jurídico ya definido que no requiere ser redefinido.

Las características del consentimiento, es decir, "libre, expreso, previo e informado" deberían estar definidas con precisión y claridad en la Ley.

Por otro lado, la definición de consentimiento del artículo 4.2 no especifica las formas en que podrá manifestarse dicho consentimiento, lo cual es importante a fin de mantener uniformidad y consistencia en el texto normativo y que éstas sean lo suficientemente flexibles para lograr adecuarse al entorno digital.

Al respecto, el texto constitucional del Ecuador, al referirse al derecho a la protección de datos de carácter personal, exige la autorización del titular o el mandato de la ley, para la recolección, archivo, procesamiento, distribución o su difusión, pero sin limitarlo al consentimiento expreso. (Art. 66 numeral 19 Constitución de la República del Ecuador), el cual por ende, podría ser expreso o tácito, adaptándose de esta manera al dinamismo que demanda la industria digital.

7.- Responsable de la bases de datos y responsable del tratamiento

A diferencia de lo establecido en la regulación comparada, el artículo 4 del proyecto de ley al referirse a las definiciones, recoge dos categorías de responsables de las bases de datos, a saber:

- Responsable del Tratamiento de la Información: persona natural o jurídica, pública o privada que administra el sistema de tratamiento de datos, por cuenta del Responsable del archivo.
- Responsable del Archivo: persona natural o jurídica, pública o privada, titular del archivo, custodio u operador de la información.

Paralelamente, en otros artículos, como el 6.1, 6.2 se refieren a otras categorías al Encargado del Tratamiento como sinónimo del Responsable del Tratamiento; mientras que el artículo 9.2 trae la figura del Encargado de las Bases de Datos, lo cual genera gran confusión; además ni el Encargado del Tratamiento, ni el Encargado de las Bases de Datos aparecen en las definiciones y su rol se presta a confusión frente a la función del Responsable del Tratamiento y del Responsable del Archivo.

Finalmente, se introduce una tercera categoría, el "Usuario de Datos" definido como persona natural o jurídica que realiza el tratamiento de los datos, lo cual genera aún más dudas respecto de las funciones que atañen a cada actor.

En la legislación comparada existen dos categorías claramente definidas, el responsable y el encargado de la base de datos. En aras de la simplificación y la adopción de un estándar internacional la norma ecuatoriana se recomienda manejar esas dos categorías, a fin de facilitar el manejo de términos en las relaciones contractuales internacionales, como es el caso del flujo transfronterizo de datos.

El responsable es quien debe obtener el consentimiento de los titulares de datos personales mientras que el encargado se limita a actuar bajo las directrices del titular o responsable de la base de datos

8.- Transferencia Internacional de Datos

En el Título V del proyecto de ley se establece como regla la prohibición a la transferencia de datos personales a países que no proporcionen niveles de protección de datos conforme con las normas de derecho internacional o regional en la materia.

En entornos digitales las restricciones a las transferencias internacionales de información y el comercio transfronterizo digital pueden generar efectos muy negativos para el desarrollo económico de cualquier país.

En ese sentido, la regla general debe ser promover los intercambios de información a nivel internacional salvo que existan razones fundadas y excepcionales para

exigir requisitos adicionales. En este sentido, cuando la transferencia internacional se produzca en el marco de la ejecución de relaciones contractuales para la prestación de servicios, por ejemplo, de almacenamiento en la nube, éstas deberían ser legalmente permitidas, caso contrario la normativa podría convertirse en un factor restrictivo para el crecimiento del comercio electrónico o de desventaja competitiva para las empresas.

Por otro lado, la disposición no determina cuáles son esos niveles de protección conforme las normas de derecho internacional o regional, lo cual nuevamente deja abierto un espacio incierto que no abona a la seguridad jurídica.

9.- Atribuciones de la Autoridad Nacional de Protección de Datos

El artículo 12 numeral 3 del proyecto de ley determina que la Autoridad de Protección de Datos podrá: disponer el bloqueo temporal o definitivo de los sistemas de información cuando exista un riesgo cierto de afectación de los derechos constitucionales, en caso de incurrir en infracciones contempladas en dicha ley.

En observancia a los principios jurídicos del debido proceso y al derecho a la defensa, cualquier medida orientada a bloquear el acceso a la información en sistemas informáticos como lo contempla el art. 12 numeral 3 del proyecto de ley, debe ceñirse estrictamente a las garantías previstas en el artículo 76 de la Constitución numerales 1, 2 y 7, literales l) y m); debiendo además, por las graves consecuencias y efectos que supone la adopción de una medida como tal, estar supeditada a orden expresa de juez competente y a la observancia del debido proceso.

Por otro lado, el Bloqueo Definitivo no constituye una medida preventiva sino una sanción en sí misma, la cual no se encuentra contemplada en el proyecto, contraviniendo lo previsto en el artículo 76 numeral 3 de la Constitución.

"Art. 76 No.3. Nadie podrá ser juzgado ni sancionado por un acto u omisión que, al momento de cometerse, no esté tipificado en la ley como infracción penal, administrativa o de otra naturaleza; ni se le aplicará una sanción no prevista por la Constitución o la ley. Sólo se podrá juzgar a una persona ante un juez o autoridad competente y con observancia del trámite propio de cada procedimiento. "

Finalmente, la condición de que el bloqueo se dispondrá cuando exista un riesgo cierto de afectación a los derechos constitucionales, es una declaración ambigua, que se presta a interpretación, abriendo espacios para arbitrariedades.

10.- Autoridad Nacional de Protección de Datos Personales

El Art. 11 del proyecto de ley determina que la Dirección Nacional de Registro de Datos Públicos, adscrita al Ministerio de Telecomunicaciones y de la Sociedad de la Información, será la Autoridad Nacional de Protección de Datos Personales.

En atención al carácter transversal de la protección de datos personales en una sociedad, que tiene repercusión en muchas esferas o sectores de la sociedad, no es recomendable que la Autoridad de Protección de Datos se encuentre vinculada o anexa a un sector en particular.

Adicionalmente, en aras de garantizar independencia e imparcialidad en las decisiones adoptadas por la Autoridad de Protección de Datos, es recomendable que sea un ente independiente, autónomo, que no se encuentre dentro de la estructura institucional de la Función Ejecutiva, puesto que su rol será velar y vigilar el cumplimiento de las normas de protección de datos tanto por entidades de naturaleza privada como pública, debiendo en los casos que lo ameriten imponer sanciones a instancias o instituciones, de las que la misma entidad de control, forma parte.

11.- Registro

El proyecto de Ley, Título IV, en el artículo 14 plantea la creación de un Registro de Bases de Datos, en el que deberán inscribirse todas las bases de datos o archivos de instancias públicas o privadas con fines financieros o mercantiles.

Al respecto, de la experiencia de la legislación comparada, no ha resultado claro cuál es el aporte real que trae a la protección de los datos personales de los ciudadanos la exigencia del registro; más bien, se ha convertido en una traba regulatoria que no añade mayor protección al titular del dato, así en muchas legislaciones se ha eliminado o se está evaluando el eliminarla.

Esta obligación no se establece, por ejemplo, en Canadá, Estados Unidos, México (en la ley del sector privado desde 2011 y en el proyecto de ley para el sector público se está eliminando), y el Reglamento Europeo de Protección de Datos lo eliminó (existía en la Directiva 95/4).

Adicionalmente, también conlleva una fuerte carga administrativa y altos costos para la Autoridad de Protección de Datos.

Finalmente, el artículo 16 presenta un error en la redacción: "Todas las bases" y no como aparece "Todas la base".

12.- Infracciones y Sanciones

El artículo 24 tipifica las infracciones de carácter leve y el Art. 25 las infracciones de carácter grave; sin embargo, se determinan las mismas sanciones para unas y otras sin considerar la menor o mayor afectación al bien jurídico protegido que supone el cometimiento de una infracción leve o una grave.

Por otro lado, dentro de las infracciones de carácter leve se contempla en el numeral 4: el mal manejo administrativo del archivo y tratamiento de bases de datos. Las infracciones deben estar tipificadas con claridad sin dejar lugar a dudas o interpretaciones, el mal manejo de un archivo da espacio a criterios subjetivos, lo cual propicia un clima de inseguridad jurídica.

6. Conclusiones

- Es fundamental armonizar la normativa sobre protección de datos dispersa en nuestro ordenamiento jurídico a través del proyecto de Ley.
- El que Ecuador no posea una ley de protección de datos hasta la fecha, no debe ser visto como una debilidad sino como una oportunidad para aprender de las experiencias de la legislación comparada, corrigiendo deficiencias o defectos advertidos en las leyes de la materia, superando los problemas o conflictos identificados de la aplicación práctica de las leyes en otros países y construir una ley madura, equilibrada, depurada y que se ajuste a las necesidades y realidades de nuestra sociedad.
- La Ley debe encontrar un balance entre la protección de los derechos a la intimidad y privacidad; el derecho a expresarse y ser informado; así como el fomento y desarrollo de la innovación tecnológica.
- Tanto las instancias públicas como privadas deberán evaluar los efectos y alcances de la normativa, puesto que todas aquellas entidades que, por la naturaleza de sus funciones u objeto social, en el caso de las empresas privadas, manejen datos personales deberán acatar las disposiciones contenidos en la ley, la cual establece disposiciones que demandarán una carga administrativa, costos administrativos y operativos, recursos humanos y económicos.
- La información personal que se genera en plataformas digitales es el resultado de la naturaleza ágil de las TICs y la economía digital, por esta razón la normativa debe ser integral con el objetivo de garantizar la neutralidad para innovación y la competitividad.

Con los aportes de:

Dr. Farith Simon. USFQ.
Dr. Juan Pablo Aguilar Andrade. USFQ
Dra. Janette Colamarco Ureña. LEGALTECH Asesores & Consultores
LL.M. Hugo Cahueñas Muñoz. USFQ.
Daniela Viteri. Observatorio de la Juventud para América Latina y el Caribe

RESEÑA BIOGRÁFICA DE LOS AUTORES

Juan Pablo Albán Alencastro

Juan Pablo Albán Alencastro es Abogado y Doctor en Jurisprudencia por la Pontificia Universidad Católica del Ecuador (PUCE). Posee además un título de Maestría en Derechos Humanos de la Universidad de Notre Dame, Estados Unidos. Por más de ocho años se desempeñó como Especialista Principal de la Comisión Interamericana de Derechos Humanos, donde sirvió sucesivamente como Oficial adjunto para Argentina y Perú, Oficial de Litigio ante la Corte Interamericana de Derechos Humanos, y Coordinador de la Sección Regional Andina. Anteriormente fue Director de la Clínica de Derechos Humanos y Profesor de la Facultad de Jurisprudencia de la Pontificia Universidad Católica del Ecuador. Actualmente es Profesor Tiempo Completo del Colegio de Jurisprudencia de la Universidad San Francisco de Quito y Director del Consultorio Jurídico Gratuito de la misma casa de estudios. El Dr. Albán también es Profesor de postgrado en las Universidades: Católica Santiago de Guayaquil, Andina Simón Bolívar y San Francisco de Quito; Miembro del Instituto Interamericano de Política Criminal con sede en México, consultor en derechos humanos de diversas instituciones nacionales y organismos internacionales; y fue finalista en el proceso para selección de Relator Especial para la Libertad de Expresión de la OEA.

Valeria Betancourt

Valeria Betancourt es socióloga con estudios de maestría en Comunicación y Cultura. Es una activista en el campo del internet, el desarrollo y la justicia social. Fue miembro del grupo asesor multisectorial de Naciones Unidas sobre gobernanza de internet. Actualmente es directora del programa global de políticas de internet de la Asociación para el Progreso de las Comunicaciones (APC) y su trabajo se enfoca en políticas de acceso a internet, derechos humanos en línea y gobernanza de internet. Su trabajo fue reconocido en el 2012 con el premio Trayectoria de LACNIC.

Hugo Cahueñas Muñoz

Profesor de Derecho y Relaciones Internacionales, Universidad San Francisco de Quito. Master en Derecho Internacional y Comparado, George Washington University. Maestro en Relaciones Internacionales con mención en Seguridad y Derechos Humanos, Facultad Latinoamericana de Ciencias Sociales. Especialización Superior en Gestión Ambiental International, Universidad Central del Ecuador. Abogado, PUCE.

Arturo J. Carrillo

Profesor de Derecho, Director de la Clínica de Derechos Humanos, Co Director del Proyecto sobre Libertad de Internet Global y Derechos Humanos en la Universidad George Washington University. Previamente fue Director de la Clínica de Derechos Humanos de la Universidad de Columbia, donde fue profesor para la facultad de Derecho y Henkin Senior Fellow con el Instituto de Derechos Humanos de Columbia. Antes de dedicarse a la academia, trabajó como consultor legal en la división de Derechos Humanos de ONUSAL (United Nations Observer Mission to El Salvador), además de organizaciones no gubernamentales en Colombia, su país natal, donde fue además profesor de leyes. Del 2005 al 2010, fue asesor senior de Derechos Humanos de la USAID en Colombia. Experto en Derecho Internacional Público, Información y Tecnologías de la Información y la Comunicación, Derechos Humanos, Libertad en Internet, Justicia, Derecho Humanitario, Derecho Clínico Comparado de Educación. Es autor de varias publicaciones, tanto en inglés como español, que abordan estos temas.

Andrés Delgado

Andrés Delgado, quien desde 2013 ha trabajado con diversos grupos de sociedad civil en la defensa de derechos humanos en internet. Fue parte del colectivo Internet Libre, que logró la eliminación del artículo 474, el cual permitía el espionaje masivo e indiscriminado a los ciudadanos ecuatorianos. Co-organizó el primer encuentro nacional de gobernanza de internet, llevado a cabo en CIESPAL en 2013

y en 2014, representó a Creative Commons ante la Asamblea Nacional promoviendo el acceso abierto a publicaciones científicas y la elusión de candados digitales para usos justos; esta última recomendación fue adoptada en la nueva propuesta de ley de propiedad intelectual tras primer debate. Actualmente Andrés estudia una maestría en política pública y asuntos globales en la Universidad de Columbia Británica, en Canadá. Becario de la SENESCYT.

Sophia Espinosa Coloma

Sophia Espinosa Coloma es abogada summa cum laude por la Universidad San Francisco de Quito donde fue la valedictorian de la clase del 2004. Asimismo, fue designada por el CONESUP como la mejor graduada de Derecho del Ecuador en el año 2004. Es, además, Especialista Superior en Derecho Financiero, Bursátil y Seguros por la Universidad Andina Simón Bolívar sede Ecuador. Fue becaria Fulbright en el 2007, beca con la que realizó su Máster en Propiedad Intelectual y Nuevas Tecnologías (LL.M. in Intellectual Property and Technology Law) en Washington University en St. Louis. Posteriormente fue acreedora a la Beca OEA para estudios Académicos y a la Beca otorgada por American Association of University Women (AAUW). En el 2010 obtuvo su Doctorado en Derecho en Washington University in St. Louis (Juris Scientiae Doctoris J.S.D.). Es miembro de la Barra del Estado de New York desde 2009. En lo profesional, fue abogada asociada de Jurídico Asociado Solines y consultora de Gobierno Digital. Asimismo, fue Directora de la Agenda Nacional de Conectividad de Ecuador. Durante su tiempo en el CONATEL, representó al país en varios eventos internacionales relacionados con Sociedad de la Información, Tecnologías de Información y Comunicación (TICs), y Gobierno Electrónico. Desde el 2011 se desempeña como profesora a tiempo completo en el Colegio de Jurisprudencia de la Universidad San Francisco de Quito.

Gustavo Gómez

Investigador, consultor y profesor universitario uruguayo. Experto en libertad de expresión, regulación y políticas públicas de medios de comunicación y de telecomunicaciones. Actualmente es Director Ejecutivo del Observatorio Latinoamericano de Regulación, Medios y Convergencia (OBSERVACOM). Además es profesor en la Licenciatura en Comunicación Social de la Universidad Católica del Uruguay (UCUDAL) desde 2008 y maestrando en la Maestría sobre Políticas y Gestión de Industrias Culturales en la Universidad Nacional de Quilmes, Argentina. Fue Director Nacional de Telecomunicaciones y Servicios de Comunicación Audiovisual (DINATEL) del gobierno de Uruguay y asesor de la Secretaría de la Presidencia de Uruguay en regulación y políticas públicas de medios audiovisuales y telecomunicaciones durante la Presidencia de José Mujica (2010-2014). Es consultor de organismos internacionales como UNESCO, Banco Mundial, Centro Carter y otros. Ha realizado informes y presentaciones sobre el derecho a la libertad de expresión en numerosas oportunidades ante organismos del Sistema Interamericano de Derechos Humanos.

Pier Pigozzi

Pier Pigozzi es profesor de derecho en la Universidad San Francisco de Quito, encargado del área de investigación de su Facultad de Jurisprudencia, y candidato J.S.D. (Juridicæ Scientiæ Doctor) en Notre Dame Law School (Indiana, EE.UU.) Sus áreas de interés académico son el Derecho Internacional, la aplicación del principio de interdependencia en el Derecho Internacional de los Derechos Humanos, la tradición constitucional en Latinoamérica y el derecho natural. Trabajó como investigador asociado y consejero académico en el Center for Civil and Human Rights de University of Notre Dame(2010-2012) y ocupó diferentes puestos en la Oficina del Alto Comisionado de las Naciones Unidas para los Refugiados (2008-2009), y en el Ministerio de Relaciones Exteriores (2005-2008); también cuenta con experiencia profesional ante el Sistema Interamericano de Derechos Humanos tanto en calidad de peticionario, como de perito ante la Corte Interamericana. Enseña cursos de postgrado en la Universidad Andina Simón Bolívar (Quito). Obtuvo su licenciatura en derecho en la Pontificia Universidad Católica del Ecuador (2006), su LL.M. (Legum Magister) en Derecho Internacional de los Derechos Humanos, magna cum laude, en Notre Dame Law School (2010) y ha realizado diferentes cursos de especialización en San Remo (2006), Lund y Lima (2008).

Javier Robalino Orellana

Javier Robalino Orellana es socio director de FERRERE en Ecuador, oficina en la co-preside la práctica del arbitraje. Ha sido profesor de Derecho Administrativo de la Universidad Católica de Quito y en la actualidad es profesor de derecho y coordinador del programa de postgrado administrativa e internacional en la Universidad San Francisco de Quito, así como profesor de la Maestría Derecho Empresarial por el Instituto de Derecho y Empresa INIDEM en Panamá, y profesor visitante en el Programa de Postgrado de la Universidad Carlos III de Energía en Madrid. Representa a multinacionales en la planificación de inversiones, las controversias y asuntos transfronterizos, así como en proyectos de petróleo, energía e infraestructura. Ha sido nombrado como árbitro internacional y ha representado a varios inversores en la inversión y disputas comerciales bajo los procedimientos del CIADI, la CNUDMI, CIAC y la CPI. En 2011, Robalino fue reconocido por "GAR 45 under 45" como uno de los principales profesionales en arbitraje internacional. Ha sido reconocido como un profesional líder por Chambers, IFLR, Latin Lawyer, Legal 500 y LACCA durante muchos años. Participa activamente en los campos de petróleo y la energía, la inversión internacional y el arbitraje comercial. También es asociado extranjero de King & Spalding. Se ha desempeñado como director y asesor de la Cámara de Industria, consultor de Quito y miembro del comité de reglamentación racionalización de la Oficina del Presidente de Ecuador, y asistente del presidente de la Corte Suprema de Ecuador.

Daniela Salazar Marín

Daniela Salazar es Vicedecana y profesora del Colegio de Jurisprudencia de la Universidad San Francisco de Quito. Además es docente de maestría en la Universidad Andina Simón Bolívar (sede Ecuador) y en la Universidad Nacional de San Martín (Buenos Aires). Es parte del Comité Directivo del Consorcio de Obligaciones Extraterritoriales (con sede en Heidelberg) y miembro de la Sección Académica de Ciencias Jurídicas de la Casa de la Cultura Ecuatoriana Benjamín Carrión. Recibió el título de abogada de la Universidad San Francisco de Quito y el título de maestría (LL.M) de Columbia University en Nueva York. Obtuvo una beca Fulbright y una beca Rómulo Gallegos. Trabajó como especialista en derechos humanos en la Secretaría Ejecutiva de la Comisión Interamericana de Derechos Humanos y ha sido consultora para la Oficina del Alto Comisionado De Derechos Humanos de Naciones Unidas, la UNESCO, la Comisión Interamericana de Derechos Humanos, la Cruz Roja Internacional, Human Rights Watch, el Centro de Estudios en Libertad de Expresión y Acceso a la Información, entre otros.

Farith Simon C.

Decano y profesor del Colegio de Jurisprudencia de la Universidad San Francisco de Quito en derechos humanos y de la infancia y adolescencia. Representante del Tribunal de Honor del Colegio de Abogados del Ecuador. Co-director de la Clínica Jurídica y del Centro de Mediación (Universidad San Francisco de Quito-Colegio de Jurisprudencia). Miembro del Directorio del INNFA (hasta diciembre del 2008). Consultor en temas de derechos humanos, niñez y justicia. Litigio en casos de interés público especialmente en casos de derechos humanos en tribunales locales y el Sistema Interamericano de Derechos Humanos. Trabaja en investigación de temas relacionados a derechos humanos, pluralismo jurídico, derechos de los niños y justicia (adopción, trabajo, trata de personas, trabajo infantil, impunidad y justicia, legislación), género y proceso penal. Ha trabajado en la capacitación a funcionarios públicos, profesores, educadores de niños de la calle, en temas de protección y garantía de derechos a la infancia y derecho de familia. Es co-redactor del llamado Memorándum de Montevideo "Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes". Lleva adelante defensa de casos en tribunales locales.

Juan Carlos Solines Moreno

Juan Carlos Solines Moreno es abogado y Doctor en Jurisprudencia por la Pontificia Universidad Católica del Ecuador. Obtuvo su primera maestría en Propiedad Intelectual y Nuevas Tecnologías por la George Washington University. En esa misma universidad obtuvo también su maestría en Derecho Internacional Comparado. Completó su formación académica obteniendo una maestría de Administración Pública con enfoque en gerencia pública y regulación de nuevas tecnologías en la

Escuela de Gobierno de la Universidad de Harvard. A lo largo de sus años de ejercicio profesional se ha constituido como un referente nacional en los ámbitos de Telecomunicaciones, Internet y Nuevas Tecnologías, Comunicación y Medios. En el ámbito profesional Juan Carlos se desempeña como socio principal de la firma de abogados Solines & Asociados. Ha trabajado también en firmas de abogados de Estados Unidos y del Reino Unido en el área de tecnología, telecomunicaciones, medios y entretenimiento. Fue vicepresidente legal y de desarrollo de negocios de la compañía de Internet eHealth Latin America en Washington DC, donde trabajó también para el Banco Mundial. En el sector público ha sido Presidente del Consejo Nacional de Telecomunicaciones CONATEL y Subsecretario General de la Administración Pública. Ha dictado cátedra en la Universidad San Francisco de Quito y en la UDLA en áreas de tecnología, telecomunicaciones y propiedad intelectual. También ha dictado conferencias en foros y universidades de varios países. Fue designado por Kofi Annan como uno de los 40 expertos en Internet que Naciones Unidas agrupó para diseñar alternativas para la gobernanza global de Internet, entre otras distinciones. Ha sido un activista y defensor de la libertad de expresión y comunicación en Ecuador. Fue candidato a la Vicepresidencia de Ecuador en 2013.

Alfredo Velazco

Economista con Postgrado en Marketing. Desde 1996 involucrado en el desarrollo de la presencia en la red de importantes marcas. Miembro de Usuarios Digitales, agrupación ciudadana por el libre ejercicio de los derechos en plataformas digitales. Es conferencista en eventos relacionados a internet y su impacto en la sociedad a nivel nacional e internacional. Ciudadano, colaborativo, curioso, viajando de la queja a la propuesta.

Vladimir Villalba Paredes

Vladimir Villalba Paredes es doctor en jurisprudencia por la Pontificia Universidad Católica del Ecuador y master en leyes por Georgetown University. Actualmente es Director de la Maestría en Derecho de Empresa en la Universidad San Francisco de Quito y profesor de Contratos y Mercantil-Societario en el mismo centro.

Daniela Viteri

Daniela Viteri es ex-alumna de la USFQ. Estudió Economía y Relaciones Internacionales. Desde hace dos años trabaja en temas de Internet, participó en el 8tavo y 9no Foro de gobernanza de internet para América Latina y el Caribe. Fue becaria del programa de Gobernanza de Internet YOUTH2015. Es una de las fundadoras del Observatorio de la Juventud para la región y miembro activa. Actualmente es Vocal de la Comisión interna para Relaciones Institucional así como de la Comisión de Proyección Externa.

El preámbulo de la Constitución establece el marco más general para entender el tratamiento jurídico que se da a la naturaleza en el Ecuador: la "armonía con la naturaleza" es un elemento de una nueva forma de "convivencia ciudadana", condición necesaria para alcanzar el "buen vivir", el "sumak kawsay", uno de los ejes de la Constitución del 2008. A partir de esto se pueden identificar normas constitucionales que regulan los temas de la naturaleza a partir de dos perspectivas: las que la reconocen como sujeto de derechos (perspectiva biocentrica o de la ecología profunda); y, como derechos de las personas y colectividades, constituyéndose en objetivo y límite para la actividad estatal (perspectiva antropocéntrica, de derechos humanos o ambientalista). El artículo 10, inciso segundo, establece que "La naturaleza será sujeto de aquellos derechos que le reconozca la Constitución", son tres esos derechos (artículos 71 y 72): 1) respeto integral de su existencia; 2) mantenimiento y regeneración de sus ciclos vitales, estructura, funciones y procesos evolutivos; y, 3) derecho a la restauración, como un derecho autónomo al que tienen derecho los individuos y colectivos a ser indemnizados en caso de un daño ambiental. Se concede amplia legitimación activa a toda persona, comunidad, pueblo o nacionalidad para exigir a las autoridades públicas el cumplimiento de los derechos declarados. Esta actio popularis se complementa con el establecimiento, en el artículo 399, de una tutela estatal sobre el ambiente con una corresponsabilidad de la ciudadanía en su preservación, lo que se articula, dice la norma, a través de un "sistema nacional descentralizado de gestión ambiental", que tiene a su cargo la defensoría del ambiente y la naturaleza. Al Estado se le impone obligaciones de promoción, respeto, garantía y reparación de esos derechos, estas son de carácter similar a las que nacen de los derechos humanos. De forma adicional se establece una obligación de largo plazo: la "restauración" Las normas, del capítulo sobre los derechos de la naturaleza, se completan con una obligación específica de "incentivo" y dos prohibiciones. El Estado, de acuerdo al tercer inciso del artículo 72, debe "incentivar a las personas naturales y jurídicas, y a los colectivos, para que protejan la naturaleza", se entiende que es una obligación adicional a la de promoción. Se prohíbe (i) la de apropiación de servicios ambientales, pero sin limitar su prestación, producción, uso y aprovechamiento por particulares, al determinar que estos deben ser regulados por el Estado; y, (ii) la introducción de organismos y material orgánico e inorgánico

especies, la destrucción de ecosistemas o l

de los ciclos naturales. El segundo inciso del artículo 71, contiene una norma de reenvío para aplicación e interpretación de los derechos de la naturaleza: en lo que proceda se podrán aplicar los principios constitucionales sobre los derechos y las reglas interpretación constitucional; los primeros contenidos en el artículo 11 y las segundas en el artículo 427. Se reconoce el derecho de los seres hu-

Google

Colegio de Jurisprudencia

ISBN: 978-9978-68-097-1

9 789978 680971